

# THE LEAST COMMON MULTIPLE OF CONSECUTIVE QUADRATIC PROGRESSION TERMS

SHAOFANG HONG AND GUOYOU QIAN

**ABSTRACT.** Let  $k$  be any given positive integer and let  $f(x) \in \mathbb{Z}[x]$  be any given quadratic polynomial with  $D$  as its discriminant and  $a$  as the coefficient of its quadratic term. To evaluate the least common multiple  $\text{lcm}_{0 \leq i \leq k} \{f(n+i)\}$  of any  $k+1$  consecutive terms in the quadratic progression  $\{f(n)\}_{n \in \mathbb{N}^*}$ , we define the function  $g_{k,f}(n) := \frac{\prod_{i=0}^k |f(n+i)|}{\text{lcm}_{0 \leq i \leq k} \{f(n+i)\}}$  for all positive integers  $n \in \mathbb{N}^* \setminus Z_{k,f}$ , where  $Z_{k,f} := \bigcup_{i=0}^k \{n \in \mathbb{N}^* : f(n+i) = 0\}$ . Let  $\mathcal{K}_f := \{j \in \mathbb{N}^* : D \neq a^2 j^2 \text{ for all integers } i \text{ with } 1 \leq i \leq j\}$ . In this paper, we show that  $g_{k,f}$  can be extended to a periodic arithmetic function if and only if  $\mathcal{K}_f$  is nonempty and  $k \in \mathcal{K}_f$ . To determine the smallest period of the extended periodic function  $g_{k,f}$ , we first study the roots of quadratic congruences. We introduce the minimal distance among the roots and develop some arithmetic properties. Subsequently, we provide detailed  $p$ -adic analysis of  $g_{k,f}$  and with the help of arithmetic properties of the minimal distance, we determine the local periods, and finally arrive at the determination of the exact value of the smallest period of  $g_{k,f}$ . In addition, we obtain asymptotic formulae of  $\log \text{lcm}_{0 \leq i \leq k} \{f(n+i)\}$  for all quadratic polynomials  $f$  as  $n$  goes to infinity. Finally, we show that the least common multiple of two or more consecutive positive integers is never a perfect power.

## 1. Introduction

The study of least common multiple of consecutive positive integers was initiated by Chebyshev [4] for the first significant attempt to prove prime number theorem. Motivated by Chebyshev's work, one naturally expects to investigate the least common multiple of consecutive terms in any given sequence of positive integers. For the least common multiple of the first  $n$  terms of a given sequence of positive integers, some results were obtained by several authors. Hanson [13] and Nair [22] got the upper bound and lower bound of  $\text{lcm}_{1 \leq i \leq n} \{i\}$  respectively. Bateman, Kalb and Stenger [2] obtained an asymptotic formula for the least common multiple of arithmetic progressions. Farhi [10] studied the least common multiple of some finite sequences of integers. Hong and Feng [15] gave the lower bound for the least common multiple of finite arithmetic progression. Recently, Hong, Qian and Tan [17] obtained an asymptotic estimate for the least common multiple of a sequence of products of linear polynomials.

Arithmetic properties of consecutive terms of any given sequence of positive integers have received many authors' attention. Let  $k$  be a fixed positive integer. Ramachandra, Shorey and Tijdeman [23] showed that if  $n, n+1, \dots, n+k-1$  are all composite numbers

---

*Date:* August 28, 2012.

*2000 Mathematics Subject Classification.* Primary 11B25, 11N13, 11A05.

*Key words and phrases.* quadratic progression, least common multiple, quadratic congruence,  $p$ -adic valuation, the smallest period.

The research was supported partially by National Science Foundation of China Grant # 10971145 and by the Ph.D. Programs Foundation of Ministry of Education of China Grant #20100181110073.

and  $(\log n)/(\log k)^2$  exceeds certain absolute constant, then the number of distinct prime divisors of  $n, n+1, \dots, n+k-1$  is at least  $k$ , which confirmed a conjecture of Grimm. In a later paper [24], they gave an answer to a stronger problem of Grimm when  $k$  belongs to a range depending on  $n$ . On the other hand, Erdős and Selfridge [9] showed that the product of two or more consecutive positive integers is never a perfect power, which confirmed a 150 years old conjecture. Subsequently, the investigation for the problem of representing perfect powers by the product of consecutive arithmetic progression terms became a common topic. There are fruitful results in this direction obtained by Bennett, Bruin, Györy, Hajdu, Pintér, Saradha, Shorey and Tijdeman. We refer readers to [3], [12], [25] and [27] for more detailed information.

Along another direction, Farhi [10] investigated the least common multiple  $\text{lcm}_{0 \leq i \leq k} \{n+i\}$  of any  $k+1$  consecutive integers, where  $k$  is a fixed positive integer. To measure the size of  $\text{lcm}_{0 \leq i \leq k} \{n+i\}$  for any positive integer  $n$ , Farhi introduced the arithmetic function  $\bar{g}_k$  defined for positive integer  $n$  by

$$\bar{g}_k(n) := \frac{\prod_{i=0}^k (n+i)}{\text{lcm}_{0 \leq i \leq k} \{n+i\}}.$$

Farhi showed that  $\bar{g}_k$  is periodic with  $k!$  as its period. Let  $\bar{P}_k$  be the smallest period of  $\bar{g}_k$ . Then  $\bar{P}_k | k!$ . At the end of [10], Farhi posed the open problem of determining the smallest period  $\bar{P}_k$ . Hong and Yang [18] improved the period  $k!$  to  $\text{lcm}_{1 \leq i \leq k} \{i\}$  and proposed a conjecture stating that  $\frac{\text{lcm}_{1 \leq i \leq k+1} \{i\}}{k+1}$  divides  $\bar{P}_k$ . Farhi and Kane [11] proved the Hong-Yang conjecture and finally determined the exact value of  $\bar{P}_k$ . Throughout, let  $\mathbb{Q}$ ,  $\mathbb{Z}$  and  $\mathbb{N}$  denote the field of rational numbers, the ring of integers and the set of nonnegative integers, respectively. Define  $\mathbb{N}^* := \mathbb{N} \setminus \{0\}$ . Let  $b \in \mathbb{N}$  and  $a, k \in \mathbb{N}^*$ . Define

$$L_k := \text{lcm}_{1 \leq i \leq k} \{i\}.$$

Hong and Qian [16] studied the least common multiple of finitely many consecutive arithmetic progression terms. Actually, they defined the arithmetic function  $g_{k,a,b} : \mathbb{N}^* \rightarrow \mathbb{N}^*$  by

$$g_{k,a,b}(n) := \frac{\prod_{i=0}^k (b + (n+i)a)}{\text{lcm}_{0 \leq i \leq k} \{b + (n+i)a\}},$$

and proved that  $g_{k,a,b}$  is periodic with the determination of the exact value of the smallest period of  $g_{k,a,b}$ .

It is well known that there are infinitely many primes in the arithmetic progression with the first term coprime to the common difference, which is due to Dirichlet [5]. While we don't know whether a similar statement holds for the primitive quadratic progression. In 1922, Hardy and Littlewood [14] provided a relevant qualitative conjecture. The Hardy-Littlewood conjecture seems to be very difficult, even though the simplest case  $n^2 + 1$  is not solved yet. A very nice approximation to this conjecture is attributed to Iwaniec [20] who showed that there are infinitely many integers  $n$  such that  $h(n)$  has at most two prime factors, where  $h(n) = an^2 + bn + c$  is a primitive irreducible polynomial with  $a > 0$  and  $c \equiv 1 \pmod{2}$ . Therefore it is interesting and important to investigate arithmetic properties of quadratic progressions.

In this paper, we mainly concern with the least common multiple  $\text{lcm}_{0 \leq i \leq k} \{f(n+i)\}$  of any  $k+1$  consecutive terms in the quadratic progression  $\{f(i)\}_{i \in \mathbb{N}^*}$ , where  $k$  is a fixed positive integer and  $f(x) = ax^2 + bx + c \in \mathbb{Z}[x]$ . Associated to  $\text{lcm}_{0 \leq i \leq k} \{f(n+i)\}$ , we

define the function  $g_{k,f}$  for all positive integers  $n \in \mathbb{N}^* \setminus Z_{k,f}$  by

$$g_{k,f}(n) := \frac{\prod_{i=0}^k |f(n+i)|}{\text{lcm}_{0 \leq i \leq k} \{f(n+i)\}}, \quad (1.1)$$

where

$$Z_{k,f} := \bigcup_{i=0}^k \{n \in \mathbb{N}^* : f(n+i) = 0\}.$$

One naturally asks the following interesting question.

**Problem 1.1.** Can  $g_{k,f}$  be extended to a periodic arithmetic function and, if so, what is the smallest period of  $g_{k,f}$ ?

We suppose that  $g_{k,f}$  can be extended to a periodic arithmetic function and by  $P_{k,f}$  we denote its smallest period. We can then use  $P_{k,f}$  to give a formula for  $\text{lcm}_{0 \leq i \leq k} \{f(n+i)\}$  as follows: For any positive integer  $n$ , we have

$$\text{lcm}_{0 \leq i \leq k} \{f(n+i)\} = \frac{\prod_{i=0}^k |f(n+i)|}{g_{k,f}(\langle n \rangle_{P_{k,f}})},$$

where  $\langle n \rangle_{P_{k,f}}$  means the least positive integer congruent to  $n$  modulo  $P_{k,f}$ . Therefore it is significant to obtain the exact value of  $P_{k,f}$ .

Since  $g_{k,f}(n) = g_{k,-f}(n)$  for any  $n \in \mathbb{N}^* \setminus Z_{k,f}$ , we can assume that  $a > 0$  in the following. If  $f(x) = ax^2 + bx + c$  satisfies that  $\gcd(a, b, c) = d > 1$ , we can then easily get that

$$g_{k,f}(n) = \frac{\prod_{i=0}^k |f(n+i)|}{\text{lcm}_{0 \leq i \leq k} \{f(n+i)\}} = d^k \frac{\prod_{i=0}^k f_1(n+i)}{\text{lcm}_{0 \leq i \leq k} \{f_1(n+i)\}} = d^k g_{k,f_1},$$

where  $f_1(x) = a_1x^2 + b_1x + c_1$  with  $a_1 = a/d$ ,  $b_1 = b/d$  and  $c_1 = c/d$ . Obviously,  $g_{k,f}$  and  $g_{k,f_1}$  have the same periodicity. If they are both periodic, they have the same smallest period. That is, we have  $P_{k,f} = P_{k,f_1}$ . Thus for simplicity, we assume that  $f(x)$  is a primitive polynomial (i.e.,  $\gcd(a, b, c) = 1$ ). As usual, for any prime number  $p$ , we let  $v_p$  be the normalized  $p$ -adic valuation of  $\mathbb{Q}$ , i.e.,  $v_p(a) = b$  if  $p^b \parallel a$ . Let  $\gcd(a, b)$  denote the greatest common divisor of any integers  $a$  and  $b$ . For any real number  $x$ , by  $\lfloor x \rfloor$  we denote the largest integer no more than  $x$ .

Throughout this paper, we always let  $a \geq 1$  and  $f(x) = ax^2 + bx + c$  be any given quadratic primitive polynomial with integer coefficients, and let

$$D := b^2 - 4ac$$

be the discriminant of  $f$ . Define

$$D_4 := \frac{D}{4^{\lfloor \frac{v_2(D)}{2} \rfloor}} \quad (1.2)$$

and

$$D_p := \frac{D}{p^{v_p(D)}} \quad (1.3)$$

for any odd prime  $p$ . Then  $D_4$  is equal to  $\frac{D}{2^{v_2(D)}}$  if  $v_2(D)$  is even, and equals  $\frac{2D}{2^{v_2(D)}}$  if  $v_2(D)$  is odd. It implies that the parity of  $v_2(D)$  and  $D_4$  is reverse and  $D_4 \not\equiv 0 \pmod{4}$ . As usual, let  $\left(\frac{\cdot}{p}\right)$  denote the Legendre symbol. For any positive integer  $k$ , we define

$$B_k := \text{lcm}_{1 \leq i \leq k} \{i(a^2i^2 - D)\} \quad (1.4)$$

and

$$A_k := \frac{B_k}{\xi_2 \left( \prod_{p \neq 2, p | \gcd(a, b)} p^{v_p(B_k)} \right) \left( \prod_{p \nmid 2aD, (\frac{D}{p}) = -1} p^{v_p(B_k)} \right) \left( \prod_{p \nmid 2a, p | D} \eta_p \right)}, \quad (1.5)$$

where

$$\xi_2 = \begin{cases} 1, & \text{if } 2|a, 2 \nmid b \text{ and } v_2(k+1) < v_2(B_k), \\ 2^{2v_2(L_k)}, & \text{if } 2 \nmid a, k < 2^{\lfloor \frac{v_2(D)}{2} \rfloor} \text{ and } v_2(k+1) < v_2(L_k), \\ 2^{v_2(B_k) - \lfloor \frac{v_2(D)}{2} \rfloor}, & \text{if } 2 \nmid a, k \geq 2^{\lfloor \frac{v_2(D)}{2} \rfloor}, D_4 \not\equiv 1 \pmod{8} \text{ and } v_2(k+1) < \lfloor \frac{v_2(D)}{2} \rfloor, \\ 2^{v_2(D)+1}, & \text{if } 2 \nmid a, k \geq 2^{\lfloor \frac{v_2(D)}{2} \rfloor} \text{ and } D_4 \equiv 1 \pmod{8}, \\ 2^{v_2(B_k)}, & \text{otherwise} \end{cases} \quad (1.6)$$

and

$$\eta_p = \begin{cases} p^{2v_p(L_k)}, & \text{if } k < p^{\lfloor \frac{v_p(D)}{2} \rfloor} \text{ and } v_p(k+1) < v_p(L_k), \\ p^{v_p(B_k) - \lceil \frac{v_p(D)}{2} \rceil}, & \text{if } k \geq p^{\lceil \frac{v_p(D)}{2} \rceil}, v_p(k+1) < \lceil \frac{v_p(D)}{2} \rceil \\ & \text{and either } 2 \nmid v_p(D) \text{ or } (\frac{D_p}{p}) = -1, \\ p^{v_p(D)}, & \text{if } k \geq p^{\lceil \frac{v_p(D)}{2} \rceil}, v_p(k+1) < v_p(B_k) - v_p(D), \\ & 2|v_p(D) \text{ and } (\frac{D_p}{p}) = 1, \\ p^{v_p(B_k)}, & \text{otherwise.} \end{cases} \quad (1.7)$$

Associated to  $f$ , we define a subset  $\mathcal{K}_f$  of the set  $\mathbb{N}^*$  of positive integers by

$$\mathcal{K}_f := \{j \in \mathbb{N}^* : D \neq a^2 i^2 \text{ for any integer } i \text{ such that } 1 \leq i \leq j\}.$$

Clearly  $\mathcal{K}_f$  is empty if and only if  $D = a^2$ . Furthermore,  $\mathcal{K}_f = \mathbb{N}^*$  if  $f$  is irreducible. Another example is given by: For  $m, l \in \mathbb{N}^*$ , letting  $f(x) = (x+m)(x+m+l)$ , then  $\mathcal{K}_f$  is empty if  $l = 1$ , and equals  $\{1, \dots, l-1\}$  if  $l \geq 2$ . We can now state the main result of this paper as follows.

**Theorem 1.2.** *Let  $k$  be a positive integer. Then  $g_{k,f}$  can be extended to a periodic arithmetic function if and only if  $\mathcal{K}_f$  is nonempty and  $k \in \mathcal{K}_f$ . If  $g_{k,f}$  can be extended to a periodic arithmetic function, then its smallest period is equal to  $A_k$  except that  $v_p(k+1) \geq v_p(A_k) \geq 1$  for at most one odd prime  $p$  such that either  $p|a$  and  $p \nmid b$  or  $p \nmid 2aD$  and  $(\frac{D}{p}) = 1$ , in which case its smallest period equals  $A_k/p^{v_p(A_k)}$ .*

Therefore Theorem 1.2 answers completely Problem 1.1. The proof of Theorem 1.2 relies heavily on the theory of quadratic congruence and local analysis. The main new technique is to introduce minimal distance among the roots of quadratic congruences.

This paper is organized as follows. In Section 2, we first study the structure of the roots of quadratic congruences and introduce the concept of the minimal distance among the roots of quadratic congruences. Consequently, we develop some arithmetic properties of the minimal distance. In Section 3, we show that  $g_{k,f}$  can be extended to a periodic arithmetic function if and only if  $\mathcal{K}_f$  is nonempty and  $k \in \mathcal{K}_f$ . Subsequently, we give a formula which factors the global period  $P_{k,f}$  into the product of the local periods  $P_{p,k,f}$ . In Section 4, we supply a detailed  $p$ -adic analysis of  $g_{k,f}$ , and with the help of the arithmetic results obtained in Section 2, we then give explicit formulae of the local periods  $P_{p,k,f}$ . In Section 5, using the results presented in Section 4, we show Theorem 1.2. Some examples are also given in Section 5 to demonstrate the validity of Theorem 1.2. In Section 6, we obtain asymptotic formulae of  $\log \text{lcm}_{0 \leq i \leq k} \{f(n+i)\}$  for all quadratic

polynomials  $f$  as  $n$  goes to infinity. In Section 7, we make some related remarks and propose some problems. In particular, we show that the least common multiple of two or more consecutive positive integers is never a perfect power as the conclusion of this paper.

## 2. Minimal distance among the roots of a quadratic congruence

Throughout this section, we let  $f(x) = ax^2 + bx + c$  be any given primitive quadratic polynomial with integer coefficients and let  $p$  denote a prime. A natural question is to determine the roots of the congruence  $f(x) \equiv 0 \pmod{p^e}$  and to investigate the relation among distinct roots. Note that the number of roots of the congruence  $x^2 \equiv n \pmod{p^e}$  is given in [19], where  $e$  and  $n$  are positive integers such that  $p \nmid n$ . Also notice that the problem of distribution of roots of quadratic congruences to prime modulus was investigated by Duke, Friedlander, Iwaniec [6] and Toth [28]. Indeed, they proved that if  $f(x)$  is irreducible over  $\mathbb{Q}$ , then the roots are uniformly distributed as the prime modulus tends to infinity. Our concern here is the structure of the roots of the congruence  $f(x) \equiv 0 \pmod{p^e}$ .

For any given nonnegative integer  $e$ , by  $S(f, p^e)$  we denote the set of solutions  $x$  with  $1 \leq x \leq p^e$  of the congruence  $f(x) \equiv 0 \pmod{p^e}$ . Evidently,  $S(f, p^0) = \{1\}$ . Throughout, for any  $x \in \mathbb{Z}_p$ , the ring of  $p$ -adic integers, by  $\langle x \rangle_{p^e}$  we mean an integer between 1 and  $p^e$  such that  $\langle x \rangle_{p^e} \equiv x \pmod{p^e}$ . We begin with the following lemma.

**Lemma 2.1.** *Let  $e$  be a positive integer and let  $p$  be a prime such that  $p|a$ . Then  $S(f, p^e)$  is empty if  $p|b$ , and equals  $\{\langle s_p \rangle_{p^e}\}$  if  $p \nmid b$ , where  $s_p$  is the unique solution of the equation  $f(x) = 0$  in the ring  $\mathbb{Z}_p$  of  $p$ -adic integers.*

*Proof.* If  $p|a$  and  $p|b$ , then  $p \nmid c$  since  $\gcd(a, b, c) = 1$ . Hence  $f(x) \equiv c \not\equiv 0 \pmod{p}$  for any integer  $x$ . Thus  $S(f, p^e)$  is empty in this case.

If  $p|a$  and  $p \nmid b$ , then there exists a unique positive integer  $x_0 \in [1, p]$  such that  $f(x_0) \equiv bx_0 + c \equiv 0 \pmod{p}$ . On the other hand, we have  $f'(x_0) = 2ax_0 + b \equiv b \not\equiv 0 \pmod{p}$ . Then by Hensel's lemma (see, for example, [21]), there is a unique  $p$ -adic integer  $s_p$  such that  $f(s_p) = 0$  and  $s_p \equiv x_0 \pmod{p}$ . Therefore  $\langle s_p \rangle_{p^e}$  is the unique solution of  $f(x) \equiv 0 \pmod{p^e}$  in the interval  $[1, p^e]$  satisfying  $\langle s_p \rangle_{p^e} \equiv s_p \pmod{p^e}$ . This completes the proof of Lemma 2.1.  $\square$

Let  $D = b^2 - 4ac$  be the discriminant of  $f(x)$ . Then we have the following results.

**Lemma 2.2.** *Let  $a$  be an odd number and let  $D_4$  be defined as in (1.2). We denote by  $a^{-1}$  the inverse of  $a$  in the ring  $\mathbb{Z}_2$  of 2-adic integers. For any positive integer  $e$ , each of the following results is true.*

(i). *If either  $e = 2\lfloor \frac{v_2(D)}{2} \rfloor - 1$  with  $D_4 \equiv 2 \pmod{4}$  or  $e \leq 2\lfloor \frac{v_2(D)}{2} \rfloor - 2$ , then*

$$S(f, 2^e) = \left\{ \left\langle -\frac{a^{-1}b}{2} \right\rangle_{2^{\lceil e/2 \rceil}} + m2^{\lceil e/2 \rceil} : 0 \leq m < 2^{\lfloor e/2 \rfloor} \right\}.$$

(ii). *If either  $e = 2\lfloor \frac{v_2(D)}{2} \rfloor - 1$  with  $D_4 \not\equiv 2 \pmod{4}$ , or  $e = 2\lfloor \frac{v_2(D)}{2} \rfloor$  with  $D_4 \equiv 1 \pmod{4}$ , then*

$$S(f, 2^e) = \left\{ \left\langle a^{-1} \left( 2^{\frac{v_2(D)}{2}} - 1 - \frac{b}{2} \right) \right\rangle_{2^{\frac{v_2(D)}{2}}} + m2^{\frac{v_2(D)}{2}} : 0 \leq m < 2^{\lfloor e/2 \rfloor} \right\}.$$

(iii). *If either  $e = 2\lfloor \frac{v_2(D)}{2} \rfloor$  with  $D_4 \not\equiv 1 \pmod{4}$ , or  $e > 2\lfloor \frac{v_2(D)}{2} \rfloor$  with  $D_4 \not\equiv 1 \pmod{8}$ , then  $S(f, 2^e)$  is empty.*

(iv). If  $D_4 \equiv 1 \pmod{8}$  and  $e > 2\lfloor \frac{v_2(D)}{2} \rfloor = v_2(D)$ , then

$$S(f, 2^e) = \begin{cases} \{\langle x_{21} \rangle_{2^e}, \langle x_{22} \rangle_{2^e}\}, & \text{if } v_2(D) = 0, \\ \{\langle a^{-1}(\pm X_{2^e} - \frac{b}{2}) \rangle_{2^{e-\frac{v_2(D)}{2}}} + m2^{e-\frac{v_2(D)}{2}} : 0 \leq m < 2^{\frac{v_2(D)}{2}}\}, & \text{otherwise,} \end{cases}$$

where  $x_{21}$  and  $x_{22}$  are the only two solutions of  $f(x) = 0$  in the ring  $\mathbb{Z}_2$  of 2-adic integers,  $X_{2^e}$  denotes the smallest root of the congruence  $x^2 \equiv \frac{D}{4} \pmod{2^e}$  in the interval  $[1, 2^{e-\frac{v_2(D)}{2}}]$ .

*Proof.* First, one can easily deduce from  $D = b^2 - 4ac$  that  $v_2(D) = 0$  if  $b$  is odd, and  $v_2(D) \geq 2$  if  $b$  is even. So for Cases (i) and (ii), since  $e \geq 1$ , one has  $v_2(D) > 0$  and thus  $b$  should be even. If  $a$  is odd and  $b$  is even, then the congruence  $f(x) \equiv 0 \pmod{2^e}$  is equivalent to

$$\left(ax + \frac{b}{2}\right)^2 \equiv \frac{b^2 - 4ac}{4} \equiv \frac{D}{4} \pmod{2^e}.$$

(i). Let  $e = 2\lfloor \frac{v_2(D)}{2} \rfloor - 1$  with  $D_4 \equiv 2 \pmod{4}$  or  $e \leq 2\lfloor \frac{v_2(D)}{2} \rfloor - 2$ . Then  $\frac{D}{4} \equiv 0 \pmod{2^e}$ . So  $y^2 \equiv \frac{D}{4} \pmod{2^e}$  has exactly  $2^{\lfloor e/2 \rfloor}$  solutions:  $m \cdot 2^{\lfloor e/2 \rfloor}$ , where  $1 \leq m \leq 2^{\lfloor e/2 \rfloor}$ . Hence we can derive from  $(ax + \frac{b}{2})^2 \equiv \frac{D}{4} \pmod{2^e}$  that  $ax + \frac{b}{2} \equiv m2^{\lfloor e/2 \rfloor} \pmod{2^e}$ , which implies that

$$x \equiv a^{-1}(m2^{\lfloor e/2 \rfloor} - \frac{b}{2}) \equiv -\frac{a^{-1}b}{2} + a^{-1}m2^{\lfloor e/2 \rfloor} \pmod{2^e}$$

with  $0 \leq m < 2^{\lfloor e/2 \rfloor}$ . Since  $a^{-1}m$  runs over a complete residue system modulo  $2^{\lfloor e/2 \rfloor}$  as  $m$  does, we get

$$x \equiv \left\langle -\frac{a^{-1}b}{2} \right\rangle_{2^{\lfloor e/2 \rfloor}} + m2^{\lfloor e/2 \rfloor} \pmod{2^e}$$

with  $0 \leq m < 2^{\lfloor e/2 \rfloor}$ . Moreover, we have

$$\left\langle -\frac{a^{-1}b}{2} \right\rangle_{2^{\lfloor e/2 \rfloor}} + m_1 2^{\lfloor e/2 \rfloor} \not\equiv \left\langle -\frac{a^{-1}b}{2} \right\rangle_{2^{\lfloor e/2 \rfloor}} + m_2 2^{\lfloor e/2 \rfloor} \pmod{2^e}$$

for any two integers  $m_1$  and  $m_2$  satisfying  $0 \leq m_1 \neq m_2 < 2^{\lfloor e/2 \rfloor}$ . So we arrive at the desired result. Thus Part (i) is proved.

(ii). Let  $e = 2\lfloor \frac{v_2(D)}{2} \rfloor - 1$  with  $D_4 \not\equiv 2 \pmod{4}$  or  $e = 2\lfloor \frac{v_2(D)}{2} \rfloor$  with  $D_4 \equiv 1 \pmod{4}$ . Then  $v_2(D)$  is even. From  $(ax + \frac{b}{2})^2 \equiv \frac{D}{4} \pmod{2^e}$  we deduce that

$$ax + \frac{b}{2} \equiv (2m+1)2^{\frac{v_2(D)}{2}-1} \pmod{2^e}$$

with  $0 \leq m < 2^{\lfloor e/2 \rfloor}$ . Thus

$$x \equiv a^{-1}\left((2m+1)2^{\frac{v_2(D)}{2}-1} - \frac{b}{2}\right) \equiv a^{-1}\left(2^{\frac{v_2(D)}{2}-1} - \frac{b}{2}\right) + a^{-1}m2^{\frac{v_2(D)}{2}} \pmod{2^e}$$

for  $0 \leq m < 2^{\lfloor e/2 \rfloor}$ . Similarly as in (i), we get

$$x \equiv \left\langle a^{-1}\left(2^{\frac{v_2(D)}{2}-1} - \frac{b}{2}\right) \right\rangle_{2^{\frac{v_2(D)}{2}}} + m2^{\frac{v_2(D)}{2}} \pmod{2^e}$$

with  $0 \leq m < 2^{\lfloor e/2 \rfloor}$ . On the other hand,

$$\left\langle a^{-1}\left(2^{\frac{v_2(D)}{2}-1} - \frac{b}{2}\right) \right\rangle_{2^{\frac{v_2(D)}{2}}} + m_1 2^{\frac{v_2(D)}{2}} \not\equiv \left\langle a^{-1}\left(2^{\frac{v_2(D)}{2}-1} - \frac{b}{2}\right) \right\rangle_{2^{\frac{v_2(D)}{2}}} + m_2 2^{\frac{v_2(D)}{2}} \pmod{2^e}.$$

for any two integers  $0 \leq m_1 \neq m_2 < 2^{\lfloor e/2 \rfloor}$ . Thus the required result follows. So part (ii) is proved.

(iii). Let  $e = 2\lfloor \frac{v_2(D)}{2} \rfloor$  with  $D_4 \not\equiv 1 \pmod{4}$  or  $e > 2\lfloor \frac{v_2(D)}{2} \rfloor$  with  $D_4 \not\equiv 1 \pmod{8}$ . If  $v_2(D) = 0$ , then we can derive from  $D_4 = D = b^2 - 4ac \not\equiv 1 \pmod{8}$  that  $b$  and  $c$  are both odd numbers. Thus for any positive integer  $n$ ,  $f(n) \not\equiv 0 \pmod{2}$ . This infers that  $S(f, 2^e)$  is empty.

If  $v_2(D) \geq 2$ , since  $e = 2\lfloor \frac{v_2(D)}{2} \rfloor$  with  $D_4 \not\equiv 1 \pmod{4}$  or  $e > 2\lfloor \frac{v_2(D)}{2} \rfloor$  with  $D_4 \not\equiv 1 \pmod{8}$ , then  $y^2 \equiv D_4 \pmod{2^{e-2\lfloor \frac{v_2(D)}{2} \rfloor+2}}$  has no solution. Hence there is no integer  $y$  satisfying  $y^2 \equiv \frac{D}{4} \pmod{2^e}$ . Thus  $(ax + \frac{b}{2})^2 \equiv \frac{D}{4} \pmod{2^e}$  has no solution, which means that  $S(f, 2^e)$  is empty. This concludes part (iii).

(iv). Let  $e > 2\lfloor \frac{v_2(D)}{2} \rfloor$  and  $D_4 \equiv 1 \pmod{8}$ . If  $v_2(D) = 0$ , then it follows from  $D_4 \equiv 1 \pmod{8}$  that  $b$  is odd and  $c$  is even. Thus one has that  $f(0) \equiv 0 \pmod{2}$  and  $f(1) \equiv 0 \pmod{2}$ . On the other hand,  $f'(0) \equiv f'(1) \equiv b \not\equiv 0 \pmod{2}$ . So by Hensel's lemma, there are exactly two 2-adic integers  $x_{21}$  and  $x_{22}$  such that  $x_{21} \equiv 0 \pmod{2}$ ,  $x_{22} \equiv 1 \pmod{2}$  and  $f(x_{21}) = f(x_{22}) = 0$ . Thus  $\langle x_{21} \rangle_{2^e}$  and  $\langle x_{22} \rangle_{2^e}$  are exactly two solutions of the congruence  $f(x) \equiv 0 \pmod{2^e}$  in the interval  $[1, 2^e]$ .

If  $v_2(D) \geq 2$ , then  $b$  is even. By the definition of  $D_4$ , we know that  $v_2(D)$  is even if  $D_4 \equiv 1 \pmod{8}$ . Since  $D_4 \equiv 1 \pmod{8}$  and  $e > 2\lfloor \frac{v_2(D)}{2} \rfloor = v_2(D)$ , it is known (see Theorem 5.1 of page 44 in [19]) that  $y^2 \equiv D_4 \pmod{2^{e+2-v_2(D)}}$  has just four solutions in the interval  $[1, 2^{e+2-v_2(D)}]$ . Let  $y_1$  denote the smallest solution in the interval  $[1, 2^{e+2-v_2(D)}]$  of  $y^2 \equiv D_4 \pmod{2^{e+2-v_2(D)}}$ . Evidently,  $y_1$  is odd and  $y_1 \in [1, 2^{e-v_2(D)}]$ . Then the four solutions of  $y^2 \equiv D_4 \pmod{2^{e+2-v_2(D)}}$  are as follows:

$$y_1, 2^{e+1-v_2(D)} - y_1, y_1 + 2^{e+1-v_2(D)}, 2^{e+2-v_2(D)} - y_1.$$

Thus the congruence

$$y^2 \equiv \frac{D}{4} \equiv 2^{v_2(D)-2} D_4 \pmod{2^e}$$

has the following solutions:

$$y = 2^{\frac{v_2(D)}{2}-1} (y_1 + m_1 2^{e-v_2(D)+1}) = 2^{\frac{v_2(D)}{2}-1} y_1 + m_1 2^{e-\frac{v_2(D)}{2}}$$

or

$$y = 2^{\frac{v_2(D)}{2}-1} (2^{e-v_2(D)+1} - y_1 + m_2 2^{e-v_2(D)+1}) = 2^{e-\frac{v_2(D)}{2}} - 2^{\frac{v_2(D)}{2}-1} y_1 + m_2 2^{e-\frac{v_2(D)}{2}},$$

where  $0 \leq m_1, m_2 < 2^{\frac{v_2(D)}{2}}$  are integers. Now let  $X_{2^e} = 2^{\frac{v_2(D)}{2}-1} y_1$ . Then from

$$(ax + \frac{b}{2})^2 \equiv \frac{D}{4} \equiv 2^{v_2(D)-2} D_4 \pmod{2^e}$$

we get that

$$ax + \frac{b}{2} \equiv \pm X_{2^e} + m 2^{e-\frac{v_2(D)}{2}} \pmod{2^e},$$

which implies that

$$x \equiv \langle a^{-1}(\pm X_{2^e} - \frac{b}{2}) \rangle_{2^{e-\frac{v_2(D)}{2}}} + a^{-1} m 2^{e-\frac{v_2(D)}{2}} \pmod{2^e}$$

for any integer  $m$  with  $0 \leq m < 2^{\frac{v_2(D)}{2}}$ . Since  $a^{-1}m$  runs over a complete residue system modulo  $2^{\frac{v_2(D)}{2}}$  as  $m$  does so, we obtain that

$$x \equiv \langle a^{-1}(\pm X_{2^e} - \frac{b}{2}) \rangle_{2^{e-\frac{v_2(D)}{2}}} + m 2^{e-\frac{v_2(D)}{2}} \pmod{2^e}$$

for any integer  $m$  with  $0 \leq m < 2^{\frac{v_2(D)}{2}}$ . One can easily check that all the  $2^{\frac{v_2(D)}{2}+1}$  elements of the set  $\{\langle a^{-1}(\pm X_{2^e} - \frac{b}{2}) \rangle_{2^{e-\frac{v_2(D)}{2}}} + m 2^{e-\frac{v_2(D)}{2}} : 0 \leq m < 2^{\frac{v_2(D)}{2}}\}$  are pairwise

incongruent modulo  $2^e$ . Thus the desired result follows immediately. The proof of Lemma 2.2 is complete.  $\square$

**Lemma 2.3.** *Let  $p$  be an odd prime with  $p \nmid a$ , and let  $D_p$  be defined as in (1.3). By  $(2a)^{-1}$  we denote the inverse of  $2a$  in the ring  $\mathbb{Z}_p$  of  $p$ -adic integers. For any positive integer  $e$ , each of the following results is true.*

(i). *If  $e \leq v_p(D)$ , then*

$$S(f, p^e) = \left\{ \langle -(2a)^{-1}b \rangle_{p^{\lceil e/2 \rceil}} + mp^{\lceil e/2 \rceil} : 0 \leq m < p^{\lceil e/2 \rceil} \right\}.$$

(ii). *If  $e > v_p(D)$  with either  $v_p(D)$  being odd or  $(\frac{D_p}{p}) = -1$ , then  $S(f, p^e)$  is empty.*

(iii). *If  $e > v_p(D)$  with  $v_p(D)$  being even and  $(\frac{D_p}{p}) = 1$ , then*

$$S(f, p^e) = \left\{ \left\langle (2a)^{-1}(\pm X_{p^e} - b) \right\rangle_{p^{e - \frac{v_p(D)}{2}}} + mp^{e - \frac{v_p(D)}{2}} : 0 \leq m < p^{\frac{v_p(D)}{2}} \right\},$$

where  $X_{p^e}$  is the smallest solution of  $x^2 \equiv D \pmod{p^e}$  in the interval  $[1, p^{e - \frac{v_p(D)}{2}}]$ .

*Proof.* Since  $p \nmid 2a$ , the congruence  $f(x) \equiv 0 \pmod{p^e}$  is equivalent to the congruence

$$(2ax + b)^2 \equiv D \pmod{p^e}. \quad (2.1)$$

(i). Let  $e \leq v_p(D)$ . Then the congruence (2.1) is equivalent to

$$2ax + b \equiv mp^{\lceil e/2 \rceil} \pmod{p^e} \quad (2.2)$$

for some integers  $1 \leq m \leq p^{\lceil e/2 \rceil}$ . From (2.2) one gets  $x \equiv (2a)^{-1}(mp^{\lceil e/2 \rceil} - b) \pmod{p^e}$  for  $1 \leq m \leq p^{\lceil e/2 \rceil}$ . Moreover, we have

$$(2a)^{-1}(m_1 p^{\lceil e/2 \rceil} - b) \not\equiv (2a)^{-1}(m_2 p^{\lceil e/2 \rceil} - b) \pmod{p^e}$$

for any two integers  $m_1$  and  $m_2$  with  $1 \leq m_1 \neq m_2 \leq p^{\lceil e/2 \rceil}$ . On the other hand, since  $(2a)^{-1}m$  runs over a complete residue system modulo  $p^{\lceil e/2 \rceil}$  as  $m$  does, we get that

$$x \equiv \langle -(2a)^{-1}b \rangle_{p^{\lceil e/2 \rceil}} + mp^{\lceil e/2 \rceil} \pmod{p^e}$$

with  $0 \leq m < p^{\lceil e/2 \rceil}$ . Thus we derive the required result immediately.

(ii). Let  $e > v_p(D)$  with either  $v_p(D)$  odd or  $(\frac{D_p}{p}) = -1$ . Suppose that there is an integer  $n_0$  such that  $n_0^2 \equiv D \pmod{p^e}$ . Then  $n_0^2 \equiv p^{v_p(D)} D_p \pmod{p^e}$ . Since  $e > v_p(D)$ ,  $p^{\lceil \frac{v_p(D)}{2} \rceil}$  divides  $n_0$ .

If  $v_p(D)$  is odd, then

$$n_0^2 \equiv p^{v_p(D)+1} \frac{n_0^2}{p^{v_p(D)+1}} \equiv p^{v_p(D)} D_p \pmod{p^e}.$$

Hence

$$p \cdot \frac{n_0^2}{p^{v_p(D)+1}} \equiv D_p \pmod{p^{e-v_p(D)}},$$

which is a contradiction.

If  $v_p(D)$  even and  $(\frac{D_p}{p}) = -1$ , then we have

$$\left( \frac{n_0}{p^{v_p(D)/2}} \right)^2 \equiv D_p \pmod{p^{e-v_p(D)}},$$

which is impossible since  $(\frac{D_p}{p}) = -1$ . Thus there is no integer  $y$  such that  $y^2 \equiv D \pmod{p^e}$ . It follows immediately that the congruence  $(2ax + b)^2 \equiv D \pmod{p^e}$  has no solution and  $S(f, p^e)$  is empty.



(iii). Let  $e > v_p(D)$  with  $v_p(D)$  even and  $(\frac{D_p}{p}) = 1$ . Then by Hensel's lemma, the congruence  $y^2 \equiv D_p \pmod{p^{e-v_p(D)}}$  has exactly two solutions  $y_0$  and  $p^{e-v_p(D)} - y_0$  in the interval  $[1, p^{e-v_p(D)}]$ . Thus for all integers  $0 \leq m < p^{\frac{v_p(D)}{2}}$ ,

$$y = p^{\frac{v_p(D)}{2}}(y_0 + mp^{e-v_p(D)}) = p^{\frac{v_p(D)}{2}}y_0 + mp^{e-\frac{v_p(D)}{2}}$$

and

$$y = p^{e-\frac{v_p(D)}{2}} - p^{\frac{v_p(D)}{2}}y_0 + mp^{e-\frac{v_p(D)}{2}},$$

are solutions of the congruence  $y^2 \equiv D \pmod{p^e}$ . Let now  $X_{p^e} = p^{\frac{v_p(D)}{2}}y_0$ . Then from (2.1), we derive that

$$2ax + b \equiv \langle \pm X_{p^e} \rangle_{p^{e-\frac{v_p(D)}{2}}} + mp^{e-\frac{v_p(D)}{2}} \pmod{p^e}.$$

Since  $(2a)^{-1}m$  runs over the complete residue system as  $m$  does, we get

$$x \equiv \left\langle (2a)^{-1}(\pm X_{p^e} - b) \right\rangle_{p^{e-\frac{v_p(D)}{2}}} + mp^{e-\frac{v_p(D)}{2}} \pmod{p^e}$$

where  $0 \leq m < p^{\frac{v_p(D)}{2}}$ . Obviously, any two class of the above  $2p^{\frac{v_p(D)}{2}}$  residue classes are distinct modulo  $p^e$ . This concludes the desired result. Lemma 2.3 is proved.  $\square$

Once we determine the set of solutions of the congruence  $f(x) \equiv 0 \pmod{p^e}$ , we naturally want to know more about these solutions. First, we introduce the following concepts, which are important ingredients in process of determining the local periods.

**Definition 2.4.** Let  $e$  be a nonnegative integer. If  $S(f, p^e)$  is nonempty, then for any  $x_1, x_2 \in S(f, p^e)$ , we define the *distance*, denoted by  $d(x_1, x_2)$ , of  $x_1$  and  $x_2$  by

$$d_{p^e}(x_1, x_2) := \min\{\langle x_1 - x_2 \rangle_{p^e}, \langle x_2 - x_1 \rangle_{p^e}\}.$$

Clearly, for any  $x_1, x_2 \in S(f, p^e)$ ,  $d_{p^e}(x_1, x_2)$  equals  $\min\{|x_1 - x_2|, p^e - |x_1 - x_2|\}$  if  $x_1 \neq x_2$ , and is  $p^e$  if  $x_1 = x_2$ .

**Definition 2.5.** Let  $e$  be a nonnegative integer. We define the *minimal distance*, denoted by  $d_{p^e}$ , among the solutions of the congruence  $f(x) \equiv 0 \pmod{p^e}$  as follows:  $d_{p^0} := 1$ , and for  $e \geq 1$ ,

$$d_{p^e} := \begin{cases} \min\{d_{p^e}(x_i, x_j) : x_i, x_j \in S(f, p^e)\}, & \text{if } S(f, p^e) \text{ is nonempty,} \\ \infty, & \text{if } S(f, p^e) \text{ is empty.} \end{cases}$$

In what follows, we study the arithmetic properties of the minimal distance  $d_{p^e}$ .

**Lemma 2.6.** Let  $S(f, p^e)$  be nonempty. Then there exists a positive integer  $n$  such that  $v_p(f(n)) \geq e$  and  $v_p(f(n + d_{p^e})) \geq e$ . Further, if  $d_{p^e} < d_{p^{e+1}}$ , then there is a positive integer  $m$  such that  $v_p(f(m)) = e$ .

*Proof.* First let  $|S(f, p^e)| = 1$ . Then  $S(f, p^e)$  contains only one element, saying  $x_0$ , and  $d_{p^e} = p^e$ . Thus one can pick  $n = x_0$  to arrive at the desired result. Lemma 2.6 is true in this case.

Now let  $|S(f, p^e)| \geq 2$ . Then by Definitions 2.5 and 2.4, there are  $x_1, x_2 \in S(f, p^e)$  with  $x_1 < x_2$  such that  $d_{p^e} = d_{p^e}(x_1, x_2)$ . It follows that

$$d_{p^e} = \min(x_2 - x_1, p^e + x_1 - x_2). \quad (2.3)$$

If  $x_2 - x_1 \leq \frac{1}{2}p^e$ , by (2.3) we have  $d_{p^e} = x_2 - x_1$ . Take  $n = x_1$ . Then we have  $v_p(f(n)) = v_p(f(x_1)) \geq e$  and  $v_p(f(n + d_{p^e})) = v_p(f(x_2)) \geq e$  as required.

If  $x_2 - x_1 > \frac{1}{2}p^e$ , then by (2.3) we have  $d_{p^e} = p^e + x_1 - x_2$ . Hence taking  $n = x_2$  gives that  $n + d_{p^e} = x_1 + p^e$ . But  $f(x_1 + p^e) \equiv f(x_1) \pmod{p^e}$  and  $f(x_1) \equiv 0 \pmod{p^e}$ . So we have  $f(n + d_{p^e}) \equiv 0 \pmod{p^e}$ . The first part of Lemma 2.6 is proved.

Now suppose that  $d_{p^e} < d_{p^{e+1}}$ . Since  $S(f, p^e)$  is nonempty, by the first part we can find a positive integer  $n_1$  such that  $v_p(f(n_1)) \geq e$  and  $v_p(f(n_1 + d_{p^e})) \geq e$ . Suppose that  $v_p(f(n_1)) > e$  and  $v_p(f(n_1 + d_{p^e})) > e$ . Then  $v_p(f(n_1)) \geq e+1$  and  $v_p(f(n_1 + d_{p^e})) \geq e+1$ . Thus  $v_p(f(\langle n_1 \rangle_{p^{e+1}})) \geq e+1$  and  $v_p(f(\langle n_1 + d_{p^e} \rangle_{p^{e+1}})) \geq e+1$ . That is,  $\langle n_1 \rangle_{p^{e+1}}$  and  $\langle n_1 + d_{p^e} \rangle_{p^{e+1}}$  are belonging to the set  $S(f, p^{e+1})$ . Since  $\langle n_1 + d_{p^e} \rangle_{p^{e+1}} - \langle n_1 \rangle_{p^{e+1}} \equiv d_{p^e} \pmod{p^{e+1}}$ , we get that  $|\langle n_1 + d_{p^e} \rangle_{p^{e+1}} - \langle n_1 \rangle_{p^{e+1}}| = d_{p^e}$  or  $p^{e+1} - d_{p^e}$ . It then follows that

$$d_{p^{e+1}} \leq d_{p^{e+1}}(\langle n_1 \rangle_{p^{e+1}}, \langle n_1 + d_{p^e} \rangle_{p^{e+1}}) = \min(d_{p^e}, p^{e+1} - d_{p^e}) \leq d_{p^e}$$

which contradicts with the assumption  $d_{p^e} < d_{p^{e+1}}$ . Therefore we have either  $v_p(f(n_1)) = e$  or  $v_p(f(n_1 + d_{p^e})) = e$ . This concludes Lemma 2.6.  $\square$

**Lemma 2.7.** *For any given prime number  $p$ , the sequence  $\{d_{p^e}\}_{e=0}^\infty$  is nondecreasing. That is,  $d_{p^0} \leq d_p \leq d_{p^2} \leq \dots \leq d_{p^e} \leq \dots$*

*Proof.* To prove Lemma 2.7, it is enough to prove  $d_{p^{e+1}} \geq d_{p^e}$  for any nonnegative integer  $e$ . Let  $e$  be any given nonnegative integer. If  $S(f, p^{e+1})$  is empty, since  $d_{p^{e+1}} = \infty$ , we have  $d_{p^{e+1}} \geq d_{p^e}$  as desired. In what follows we assume that  $S(f, p^{e+1})$  is not empty.

Clearly, it suffices to prove that  $d_{p^{e+1}}(x_1, x_2) \geq d_{p^e}$  for any two elements  $x_1, x_2 \in S(f, p^{e+1})$ , from which we derive that  $d_{p^{e+1}} \geq d_{p^e}$ . Taking any two elements  $x_1, x_2 \in S(f, p^{e+1})$ , then we have that  $x_1 = y_1 + t_1 p^e$  and  $x_2 = y_2 + t_2 p^e$  for some integers  $t_1, t_2, y_1, y_2$  with  $0 \leq t_1, t_2 \leq p-1$  and  $y_1, y_2 \in S(f, p^e)$ . It is clear that

$$d_{p^{e+1}}(x_1, x_2) = \min\{\langle (t_1 - t_2)p^e \rangle_{p^{e+1}}, \langle (t_2 - t_1)p^e \rangle_{p^{e+1}}\} \geq p^e = d_{p^e}(y_1, y_2) \geq d_{p^e}$$

if  $y_1 = y_2$ . Let now  $y_1 \neq y_2$ . Then  $x_1 \neq x_2$ . We have

$$d_{p^{e+1}}(x_1, x_2) = \min\{|y_1 - y_2 + (t_1 - t_2)p^e|, p^{e+1} - |y_1 - y_2 + (t_1 - t_2)p^e|\}$$

and

$$d_{p^e}(y_1, y_2) = \min\{|y_1 - y_2|, p^e - |y_1 - y_2|\}.$$

If  $t_1 = t_2$ , then  $d_{p^{e+1}}(x_1, x_2) = |y_1 - y_2| \geq d_{p^e}(y_1, y_2) \geq d_{p^e}$ .

If  $t_1 \neq t_2$ , then we have

$$|y_1 - y_2 + (t_1 - t_2)p^e| \geq |(t_1 - t_2)p^e| - |y_1 - y_2| \geq p^e - |y_1 - y_2| \geq d_{p^e}(y_1, y_2) \geq d_{p^e}$$

and

$$\begin{aligned} p^{e+1} - |y_1 - y_2 + (t_1 - t_2)p^e| &\geq p^{e+1} - |y_1 - y_2| - |(t_1 - t_2)p^e| \\ &\geq p^e - |y_1 - y_2| \geq d_{p^e}(y_1, y_2) \geq d_{p^e}. \end{aligned}$$

It follows that  $d_{p^{e+1}}(x_1, x_2) \geq d_{p^e}$ . So Lemma 2.7 is proved.  $\square$

**Lemma 2.8.** *If  $p|a$ , then for any positive integer  $e$ , we have*

$$d_{p^e} = \begin{cases} \infty, & \text{if } p|b, \\ p^e, & \text{if } p \nmid b. \end{cases}$$

*Proof.* It follows immediately from Lemma 2.1 that Lemma 2.8 is true.  $\square$

**Lemma 2.9.** *Let  $a$  be odd and  $e$  be a positive integer.*

(i). *If  $e = v_2(D)$  with  $D_4 \equiv 1 \pmod{4}$  or  $e \leq 2\lfloor \frac{v_2(D)}{2} \rfloor - 1$ , then  $d_{2^e} = 2^{\lceil e/2 \rceil}$ . Also  $d_{2^e}$  equals the smallest positive root of  $a^2x^2 - D \equiv 0 \pmod{2^e}$ . Moreover, the distance between any two distinct solutions of  $f(x) \equiv 0 \pmod{2^e}$  is divisible by  $2^{\lceil e/2 \rceil}$  if  $e \geq 2$ .*

(ii). *If  $e = 2\lfloor \frac{v_2(D)}{2} \rfloor$  with  $D_4 \not\equiv 1 \pmod{4}$  or  $e > 2\lfloor \frac{v_2(D)}{2} \rfloor$  with  $D_4 \not\equiv 1 \pmod{8}$ , then  $d_{2^e} = \infty$ .*

(iii). *If  $e > 2\lfloor \frac{v_2(D)}{2} \rfloor = v_2(D)$  with  $D_4 \equiv 1 \pmod{8}$ , then  $d_{2^e}$  is equal to the smallest positive root of the congruence  $a^2x^2 - D \equiv 0 \pmod{2^{e+1}}$ .*

*Proof.* (i). It is easy to check that  $d_{2^e} = 2^e = 2^{\lceil e/2 \rceil}$  if  $e = 1$ . So it is enough to prove part (i) for the case  $e \geq 2$ . In what follows we let  $e \geq 2$ .

If  $e = 2\lfloor \frac{v_2(D)}{2} \rfloor - 1$  with  $D_4 \equiv 2 \pmod{4}$  or  $e \leq 2\lfloor \frac{v_2(D)}{2} \rfloor - 2$ , then by Lemma 2.2 (i),  $\langle -\frac{a^{-1}b}{2} \rangle_{2^{\lceil e/2 \rceil}} + i2^{\lceil e/2 \rceil}$  and  $\langle -\frac{a^{-1}b}{2} \rangle_{2^{\lceil e/2 \rceil}} + j2^{\lceil e/2 \rceil}$  are two roots of  $f(x) \equiv 0 \pmod{2^e}$ , where  $0 \leq i \neq j < 2^{\lceil e/2 \rceil}$ . It is easy to see that

$$\langle -\frac{a^{-1}b}{2} \rangle_{2^{\lceil e/2 \rceil}} + i2^{\lceil e/2 \rceil} - (\langle -\frac{a^{-1}b}{2} \rangle_{2^{\lceil e/2 \rceil}} + j2^{\lceil e/2 \rceil}) \equiv (i-j)2^{\lceil e/2 \rceil} \pmod{2^e}. \quad (2.4)$$

We can find two integers  $i_0$  and  $j_0$  with  $0 \leq i_0 \neq j_0 < 2^{\lceil e/2 \rceil}$  such that  $(i_0 - j_0) = 1$ . Then by (2.4), we have  $d_{2^e} = 2^{\lceil e/2 \rceil}$  as required.

If either  $e = 2\lfloor \frac{v_2(D)}{2} \rfloor - 1$  with  $D_4 \not\equiv 2 \pmod{4}$  or  $e = 2\lfloor \frac{v_2(D)}{2} \rfloor = v_2(D)$  with  $D_4 \equiv 1 \pmod{4}$ , then  $v_2(D) \geq 2$  is even in this case. For any two integers  $i$  and  $j$  with  $0 \leq i \neq j < 2^{\frac{v_2(D)}{2}}$ , we have

$$\left\langle a^{-1} \left( 2^{\frac{v_2(D)}{2}-1} - \frac{b}{2} \right) \right\rangle_{2^{\frac{v_2(D)}{2}}} + i2^{\frac{v_2(D)}{2}} - \left( \left\langle a^{-1} \left( 2^{\frac{v_2(D)}{2}-1} - \frac{b}{2} \right) \right\rangle_{2^{\frac{v_2(D)}{2}}} + j2^{\frac{v_2(D)}{2}} \right) = (i-j)2^{\frac{v_2(D)}{2}} \quad (2.5)$$

Then by Lemma 2.2 (ii), we have  $d_{2^e} = 2^{\frac{v_2(D)}{2}} = 2^{\lceil e/2 \rceil}$  as desired. Evidently, under the assumptions of part (i), we have  $e \leq v_2(D)$ . So  $2^{\lceil e/2 \rceil}$  is the smallest positive root of  $a^2x^2 - D \equiv 0 \pmod{2^e}$ . Finally, by (2.4) and (2.5),  $2^{\lceil e/2 \rceil}$  divides the distance between any two distinct solutions of  $f(x) \equiv 0 \pmod{2^e}$ .

(ii). By Lemma 2.2 (iii),  $S(f, 2^e)$  is empty in this case, which means that  $d_{2^e} = \infty$ .

(iii). Since  $D_4 \equiv 1 \pmod{8}$ ,  $v_2(D)$  is even. If  $v_2(D) = 0$ , then  $D = D_4$ . Clearly  $d_2 = 1$  is the smallest positive root of  $a^2x^2 - D \equiv 0 \pmod{2^2}$ . In what follows, we only need to consider the case either  $v_2(D) = 0$  and  $e \geq 2$ , or  $v_2(D) \geq 2$  and  $e \geq v_2(D) + 1$ .

For any integer  $x_1$  satisfying  $f(x_1) \equiv 0 \pmod{2^e}$ , we have  $(2ax_1 + b)^2 \equiv D \pmod{2^{e+2}}$ . Hence  $(2ax_1 + b)^2 \equiv D \pmod{2^{e+1}}$ . Note that the discriminant of  $x^2 - D$  equals  $4D$ . Since

$$v_2(4D) = v_2(D) + 2 \text{ and } \frac{4D}{2^{v_2(D)+2}} = D_4 \equiv 1 \pmod{8},$$

then Lemma 2.2 (iv) applied to the congruence

$$x^2 - D \equiv 0 \pmod{2^{e+1}} \quad (2.6)$$

gives exactly  $2^{\frac{v_2(D)+2}{2}+1} = 2^{\frac{v_2(D)}{2}+2}$  roots of (2.6). Now let  $y_{e+1}$  be the smallest positive root of  $a^2x^2 - D \equiv 0 \pmod{2^{e+1}}$ . Then  $y_{e+1} \in [1, 2^{e-1-v_2(D)/2})$  and  $2^{\frac{v_2(D)}{2}}$  divides  $y_{e+1}$ . We claim that the set of solutions in the interval  $[1, 2^{e+1}]$  of the congruence (2.6) is given as follows:

$$\{\langle \pm ay_{e+1} \rangle_{2^{e-\frac{v_2(D)}{2}}} + m2^{e-\frac{v_2(D)}{2}} : 0 \leq m < 2^{\frac{v_2(D)}{2}+1}\}. \quad (2.7)$$

On the one hand, since  $2^{\frac{v_2(D)}{2}}$  divides  $y_{e+1}$  and  $e > v_2(D)$ , one can easily check that each one in the set (2.7) satisfies (2.6). On the other hand, it is clear that any two elements in the set (2.7) are incongruent modulo  $2^{e+1}$  and the set (2.7) holds  $2^{\frac{v_2(D)}{2}+2}$  elements. Thus (2.7) gives all the solutions in the interval  $[1, 2^{e+1}]$  of the congruence (2.6). The claim is proved.

Now from the claim we get that

$$2ax_1 + b \equiv \pm ay_{e+1} + m_0 2^{e-\frac{v_2(D)}{2}} \pmod{2^{e+1}}$$

for some  $0 \leq m_0 < 2^{\frac{v_2(D)}{2}+1}$ , which implies that

$$2ax_1 + b \equiv ay_{e+1} \text{ or } -ay_{e+1} \pmod{2^{e-\frac{v_2(D)}{2}}}.$$

In what follows we show that  $d_{2^e} = y_{e+1}$ . Since the proof for the case  $2ax_1 + b \equiv -ay_{e+1} \pmod{2^{e-\frac{v_2(D)}{2}}}$  is similar as that of the case  $2ax_1 + b \equiv ay_{e+1} \pmod{2^{e-\frac{v_2(D)}{2}}}$ , we only treat the latter case. Let  $2ax_1 + b \equiv ay_{e+1} \pmod{2^{e-\frac{v_2(D)}{2}}}$ . Then we have

$$\begin{aligned} a(x_1 - y_{e+1})^2 + b(x_1 - y_{e+1}) + c &\equiv -(2ax_1 + b)y_{e+1} + ay_{e+1}^2 \\ &\equiv -(ay_{e+1} + t2^{e-\frac{v_2(D)}{2}})y_{e+1} + ay_{e+1}^2 \equiv -ty_{e+1}2^{e-\frac{v_2(D)}{2}} \pmod{2^e} \end{aligned}$$

for some integer  $t$ . Since  $2^{\frac{v_2(D)}{2}} \mid y_{e+1}$ , we then derive that

$$f(x_1 - y_{e+1}) \equiv -ty_{e+1}2^{e-\frac{v_2(D)}{2}} \equiv 0 \pmod{2^e}.$$

So  $x_1 - y_{e+1}$  is a solution of  $f(x) \equiv 0 \pmod{2^e}$ . But  $x_1$  is a solution of  $f(x) \equiv 0 \pmod{2^e}$ . It follows that  $d_{2^e} \leq d_{2^e}(x_1, x_1 - y_{e+1}) \leq y_{e+1}$ .

Noticing that

$$f(x_1 + m2^{e-\frac{v_2(D)}{2}}) = f(x_1) + (2ax_1 + b)m2^{e-\frac{v_2(D)}{2}} + am^2 2^{2e-v_2(D)},$$

$2^{\frac{v_2(D)}{2}} \mid (2ax_1 + b)$  and  $e > v_2(D)$ , we deduce that

$$f(x_1 + m2^{e-\frac{v_2(D)}{2}}) \equiv 0 \pmod{2^e}$$

for any integer  $m$ . Replacing  $x_1$  by  $x_1 - y_{e+1}$  gives that

$$f(x_1 - y_{e+1} + m2^{e-\frac{v_2(D)}{2}}) \equiv 0 \pmod{2^e}$$

for any integer  $m$ . Thus by Lemma 2.2 (iv), one knows that

$$\langle x_1 \rangle_{2^{e-\frac{v_2(D)}{2}}}, \langle x_1 - y_{e+1} \rangle_{2^{e-\frac{v_2(D)}{2}}}$$

are the only two distinct solutions of  $f(x) \equiv 0 \pmod{2^e}$  in the interval  $[1, 2^{e-\frac{v_2(D)}{2}}]$ .

Since

$$\langle x_1 \rangle_{2^{e-\frac{v_2(D)}{2}}} - \langle x_1 - y_{e+1} \rangle_{2^{e-\frac{v_2(D)}{2}}} \equiv y_{e+1} \pmod{2^{e-\frac{v_2(D)}{2}}},$$

one can easily check that

$$\langle x_1 \rangle_{2^{e-\frac{v_2(D)}{2}}} - \langle x_1 - y_{e+1} \rangle_{2^{e-\frac{v_2(D)}{2}}}$$

is a solution of  $a^2x^2 - D \equiv 0 \pmod{2^{e+1}}$ . It then follows immediately that so is

$$\langle \pm \langle x_1 \rangle_{2^{e-\frac{v_p(D)}{2}}} \mp \langle x_1 - y_{e+1} \rangle_{2^{e-\frac{v_p(D)}{2}}} + l2^{e-\frac{v_p(D)}{2}} \rangle_{2^e} \quad (2.8)$$

for any integer  $l$ . However, by the definition of  $d_{2^e}$  and Lemma 2.2 (iv),  $d_{2^e}$  must be of the form (2.8) for some integer  $l$ . Therefore  $d_{2^e}$  is a solution of  $a^2x^2 - D \equiv 0 \pmod{2^{e+1}}$ . Then by the minimality of  $y_{e+1}$ , we have  $d_{2^e} \geq y_{e+1}$ . So we get that  $d_{2^e} = y_{e+1}$  as desired. Part (iii) is proved.

The proof of Lemma 2.9 is complete.  $\square$

**Lemma 2.10.** *Let  $p$  be an odd prime with  $p \nmid a$ , and let  $D_p$  be defined as in (1.3).*

(i). *If  $e \leq v_p(D)$ , then  $d_{p^e} = p^{\lceil e/2 \rceil}$ . Further,  $d_{p^e}$  is equal to the smallest positive root of the congruence  $a^2x^2 - D \equiv 0 \pmod{p^e}$ . Moreover, the distance between any two distinct solutions of the congruence  $f(x) \equiv 0 \pmod{p^e}$  is divisible by  $p^{\lceil e/2 \rceil}$  if  $e \geq 2$ .*

(ii). *If  $e > v_p(D)$  with either  $v_p(D)$  being odd or  $(\frac{D_p}{p}) = -1$ , then  $d_{p^e} = \infty$ .*

(iii). *If  $e > v_p(D)$  with  $v_p(D)$  being even and  $(\frac{D_p}{p}) = 1$ , then  $d_{p^e}$  equals the smallest positive root of the congruence  $a^2x^2 - D \equiv 0 \pmod{p^e}$ .*

*Proof.* (i). Obviously, part (i) is true if  $e = 1$ . So we only need to show that part (i) holds for the case  $e \geq 2$ . Now let  $e \geq 2$ . For any given two integers  $m_1$  and  $m_2$  with  $0 \leq m_1 \neq m_2 < p^{\lceil e/2 \rceil}$ , we have

$$\langle -(2a)^{-1}b \rangle_{p^{\lceil e/2 \rceil}} + m_1p^{\lceil e/2 \rceil} - (\langle -(2a)^{-1}b \rangle_{p^{\lceil e/2 \rceil}} + m_2p^{\lceil e/2 \rceil}) \equiv (m_1 - m_2)p^{\lceil e/2 \rceil} \pmod{p^e}.$$

It is easy to derive from the above congruence and Lemma 2.3 (i) that the distance between any two distinct solutions of  $f(x) \equiv 0 \pmod{p^e}$  is divisible by  $p^{\lceil e/2 \rceil}$ .

Pick two integers  $m'_1$  and  $m'_2$  in the interval  $[0, p^{\lceil e/2 \rceil})$  such that  $m'_1 - m'_2 = 1$ . Thus  $d_{p^e} = p^{\lceil e/2 \rceil}$ . But  $e \leq v_p(D)$ . So  $p^{\lceil e/2 \rceil}$  is the smallest solution of the congruence  $a^2x^2 - D \equiv 0 \pmod{p^e}$ . Part (i) is proved.

(ii). Since  $e > v_p(D)$  with  $v_p(D)$  being odd or  $(\frac{D_p}{p}) = -1$ , by Lemma 2.3 we know that  $S(f, p^e)$  is empty. Thus  $d_{p^e} = \infty$  as desired.

(iii). Since  $e > v_p(D)$  with  $v_p(D)$  being even and  $(\frac{D_p}{p}) = 1$ , by Lemma 2.3 (iii) the congruence  $a^2x^2 - D \equiv 0 \pmod{p^e}$  has exactly  $2p^{\frac{v_p(D)}{2}}$  roots in any complete residue system modulo  $p^e$ . Let  $y_e$  be the smallest positive root of the congruence  $a^2x^2 - D \equiv 0 \pmod{p^e}$ . Then Lemma 2.3 (iii) applied to the congruence  $a^2x^2 - D \equiv 0 \pmod{p^e}$  gives that  $y_e \in [1, p^{e-\frac{v_p(D)}{2}}]$  and  $v_p(y_e) = v_p(X_{p^e}) = \frac{v_p(D)}{2}$ . One can easily check that

$$\langle ay_e \rangle_{p^{e-\frac{v_p(D)}{2}}}, \langle -ay_e \rangle_{p^{e-\frac{v_p(D)}{2}}}$$

are the only two solutions of  $x^2 - D \equiv 0 \pmod{p^e}$  in the interval  $[1, p^{e-\frac{v_p(D)}{2}}]$ . So by Lemma 2.3 (iii), the following set

$$\{ \langle \pm ay_e \rangle_{p^{e-\frac{v_p(D)}{2}}} + mp^{e-\frac{v_p(D)}{2}} : 0 \leq m < p^{\frac{v_p(D)}{2}} \} \quad (2.9)$$

is exactly the set of all the solutions of the congruence  $x^2 - D \equiv 0 \pmod{p^e}$  in the interval  $[1, p^e]$ . For any solution  $x_0$  of  $f(x_0) \equiv 0 \pmod{p^e}$ , one has  $(2ax_0 + b)^2 \equiv D \pmod{p^e}$ . By (2.9), we have  $2ax_0 + b \equiv \langle \pm ay_e \rangle_{p^{e-\frac{v_p(D)}{2}}} + mp^{e-\frac{v_p(D)}{2}} \pmod{p^e}$  for some

$0 \leq m < p^{e-\frac{v_p(D)}{2}}$ , which implies that  $2ax_0 + b \equiv ay_e$  or  $-ay_e \pmod{p^{e-\frac{v_p(D)}{2}}}$ .

Now we prove that  $d_{p^e} = y_e$ . We only need to give the the proof for the case  $2ax_0 + b \equiv ay_e \pmod{p^{e-\frac{v_p(D)}{2}}}$ , since the proof for the case  $2ax_0 + b \equiv -ay_e \pmod{2^{e-\frac{v_2(D)}{2}}}$  is similar. Let now  $2ax_0 + b \equiv ay_e \pmod{p^{e-\frac{v_p(D)}{2}}}$ . Then  $2ax_0 + b = ay_e + mp^{e-\frac{v_p(D)}{2}}$  for some integer  $m$ . Using the fact that  $v_p(y_e) = \frac{v_p(D)}{2}$ , we get

$$f(x_0 - y_e) \equiv -(2ax_0 + b)y_e + ay_e^2 \equiv 0 \pmod{p^e},$$

i.e.,  $x_0 - y_e$  is a solution of  $f(x) \equiv 0 \pmod{p^e}$ . Note that  $x_0$  is also a solution of  $f(x) \equiv 0 \pmod{p^e}$ . Therefore,  $d_{p^e} \leq d_{p^e}(x_0, x_0 - y_e) \leq y_e$ .

We can check that

$$\langle x_0 \rangle_{p^{e-\frac{v_p(D)}{2}}}, \langle x_0 - y_e \rangle_{p^{e-\frac{v_p(D)}{2}}}$$

are the only two distinct solutions of  $f(x) \equiv 0 \pmod{p^e}$  in the interval  $[1, p^{e-\frac{v_p(D)}{2}}]$ . Thus by Lemma 2.3 (iii),  $S(f, p^e)$  is equal to the following union:

$$\{\langle x_0 \rangle_{p^{e-\frac{v_p(D)}{2}}} + mp^{e-\frac{v_p(D)}{2}} : 0 \leq m < p^{\frac{v_p(D)}{2}}\} \cup \{\langle x_0 - y_e \rangle_{p^{e-\frac{v_p(D)}{2}}} + mp^{e-\frac{v_p(D)}{2}} : 0 \leq m < p^{\frac{v_p(D)}{2}}\}.$$

Then  $d_{p^e}$  must be of the form

$$\left\langle \pm \langle x_0 \rangle_{p^{e-\frac{v_p(D)}{2}}} \mp \langle x_0 - y_e \rangle_{p^{e-\frac{v_p(D)}{2}}} + mp^{e-\frac{v_p(D)}{2}} \right\rangle_{p^e}$$

for some integer  $m$ . It follows from Lemma 2.3 (iii) that  $\pm y_e + tp^{e-\frac{v_p(D)}{2}}$  is the root of  $a^2x^2 - D \equiv 0 \pmod{p^e}$  for any integer  $t$ . On the other hand, since

$$\left\langle \pm \langle x_0 \rangle_{p^{e-\frac{v_p(D)}{2}}} \mp \langle x_0 - y_e \rangle_{p^{e-\frac{v_p(D)}{2}}} + mp^{e-\frac{v_p(D)}{2}} \right\rangle_{p^e} \equiv \pm y_e \pmod{p^{e-\frac{v_p(D)}{2}}}$$

for any integer  $m$ ,  $d_{p^e}$  is a solution of  $a^2x^2 - D \equiv 0 \pmod{p^e}$ . Since  $y_e$  is the smallest positive root of the congruence  $a^2x^2 - D \equiv 0 \pmod{p^e}$ , we have  $d_{p^e} \geq y_e$ . So  $d_{p^e} = y_e$  as required. Part (iii) is proved.

This completes the proof of Lemma 2.10.  $\square$

**Lemma 2.11.** *If  $\mathcal{K}_f$  is nonempty, then we have either  $\mathcal{K}_f = \mathbb{N}^*$ , or  $\mathcal{K}_f = \{1, \dots, l\}$ , where  $l$  is an integer such that  $a^2(l+1)^2 = D$ .*

*Proof.* If  $\mathcal{K}_f = \mathbb{N}^*$ , then Lemma 2.11 is true.

If  $\mathcal{K}_f \neq \mathbb{N}^*$ , then the set  $\mathbb{N}^* \setminus \mathcal{K}_f$  is nonempty. By the well-ordering principle (see, for example, page 13 of [1]), we know that  $\mathbb{N}^* \setminus \mathcal{K}_f$  contains a smallest member, named  $s_0 = \min(\mathbb{N}^* \setminus \mathcal{K}_f)$ . So  $s_0 \notin \mathcal{K}_f$ . Suppose that  $s_0 = 1$ . Then  $1 \notin \mathcal{K}_f$  and so  $a^2 = D$ . It infers that  $\mathcal{K}_f$  is empty, which is impossible since  $\mathcal{K}_f$  is nonempty. Thus we have that  $s_0 \geq 2$  and all the integers  $s$  with  $s < s_0$  are belonging to  $\mathcal{K}_f$ , i.e.,  $\{1, \dots, s_0 - 1\} \subseteq \mathcal{K}_f$ .

On the other hand, since  $s_0 \notin \mathcal{K}_f$ , there is an integer  $s'$  with  $1 \leq s' \leq s_0$  such that  $a^2s'^2 - D = 0$ . Thus  $s' \in \mathbb{N}^* \setminus \mathcal{K}_f$ . By the minimality of  $s_0$ , one has  $s' = s_0$ . Hence  $a^2s_0^2 - D = 0$ , which implies that  $s_0 + j \notin \mathcal{K}_f$  for all nonnegative integers  $j$ . Therefore  $\mathcal{K}_f = \{1, \dots, s_0 - 1\}$  as desired.

This completes the proof of Lemma 2.11.  $\square$

Lemma 2.7 tells us that the sequence  $\{d_{p^e}\}_{e=0}^\infty$  is nondecreasing. The following result describes a condition on  $f$  which guarantees that  $\{d_{p^e}\}_{e=0}^\infty$  is not a constant sequence.

**Lemma 2.12.** *Let  $\mathcal{K}_f$  be nonempty and  $k \in \mathcal{K}_f$ . Then for any prime  $p$ , there exists a unique nonnegative integer  $e$  such that*

$$d_{p^e} \leq k < d_{p^{e+1}}.$$

*Proof.* Let  $\mathcal{K}_f$  be nonempty and  $p$  be a prime. For any  $k \in \mathcal{K}_f$ , we define the subset  $R_p(k)$  of  $\mathbb{N}^*$  by

$$R_p(k) := \{i \in \mathbb{N}^* : k < d_{p^i}\}.$$

If the set  $R_p(k)$  is nonempty, then by the well-ordering principle [1], we know that  $R_p(k)$  contains a smallest element, named  $i_0 = \min(R_p(k))$ . Letting  $e = i_0 - 1$  gives the desired result  $d_{p^e} \leq k < d_{p^{e+1}}$ . The uniqueness of  $e$  follows from Lemma 2.7. Thus we only need to show that  $R_p(k)$  is nonempty for any prime  $p$ . In the following we show the equivalent statement that there is a positive integer  $t$  such that  $k < d_{p^t}$ .

First let  $p$  be a prime such that  $p \mid a$ . If  $p \mid b$ , then one can take  $t = 1$  since by Lemma 2.8, we have  $d_{p^0} \leq k < d_p = \infty$ . If  $p \nmid b$ , then pick  $t$  to be a positive integer such that  $k < p^t$ . However, Lemma 2.8 tells us that  $d_{p^t} = p^t$ . Hence  $k < d_{p^t}$ . The statement is true for the case  $p \mid a$ .

Consequently, we let  $p$  be a prime such that  $p \nmid a$ .

If  $p = 2$  and  $D_4 \not\equiv 1 \pmod{8}$ , then we take  $t = 2\lfloor \frac{v_2(D)}{2} \rfloor + 1$ . Then by Lemma 2.9 (ii), we obtain that  $d_{2^t} = \infty$  and thus  $k < d_{2^t}$ . The statement is true in this case.

If  $p$  is an odd prime with either  $v_p(D)$  being odd or  $(\frac{D_p}{p}) = -1$ , then we take  $t = v_p(D) + 1$ . But  $d_{p^{v_p(D)+1}} = \infty$  by Lemma 2.10 (ii). So we get the desired result  $k < d_{p^t}$ . The statement is proved in this case.

If either  $p = 2$  and  $D_4 \equiv 1 \pmod{8}$ , or  $p$  is an odd prime with  $v_p(D)$  being even and  $(\frac{D_p}{p}) = 1$ , then by the assumption that  $\mathcal{K}_f$  is nonempty and Lemma 2.11, we have either  $\mathcal{K}_f = \mathbb{N}^*$ , or  $\mathcal{K}_f = \{1, \dots, l\}$  for some positive integer  $l$  satisfying  $a^2(l+1)^2 = D$ . We take

$$t = \max(v_p(D) + 1, \log_p(a^2k^2 + |D|) + 1) \quad (2.10)$$

if  $\mathcal{K}_f = \mathbb{N}^*$ , and

$$t = \max(v_p(D) + 1, \max_{1 \leq i \leq l} \{v_p(a^2i^2 - D)\}) + 1 \quad (2.11)$$

if  $\mathcal{K}_f$  is a finite set. So  $t > v_p(D)$ . It then follows from Lemma 2.9 (iii) and Lemma 2.10 (iii) that  $d_{p^t}$  is the smallest positive root of  $a^2x^2 - D \equiv 0 \pmod{p^{t+1}}$  if  $p = 2$  and  $d_{p^t}$  is the smallest positive root of  $a^2x^2 - D \equiv 0 \pmod{p^t}$  if  $p \neq 2$ , respectively. Now we show that  $d_{p^t} > k$ .

For the former case  $\mathcal{K}_f = \mathbb{N}^*$ , we have that  $a^2i^2 - D \neq 0$  for any  $i \in \mathbb{N}^*$ . By (2.10), we have  $t > v_p(D)$  and  $p^t > a^2k^2 + |D|$ . Since  $a^2d_{p^t}^2 - D \equiv 0 \pmod{p^t}$ , we can write  $a^2d_{p^t}^2 - D = p^t u$  for some integer  $u$ . Then  $u \neq 0$  because  $a^2i^2 - D \neq 0$  for any  $i \in \mathbb{N}^*$ . It then follows that  $a^2d_{p^t}^2 \geq p^t - |D| > a^2k^2$ , which implies that  $d_{p^t} > k$  as required.

For the latter case that  $\mathcal{K}_f = \{1, \dots, l\}$ , we have  $a^2(l+1)^2 - D = 0$ . But by (2.11), we have  $a^2i^2 - D \not\equiv 0 \pmod{p^t}$  for all  $1 \leq i \leq l$ . Hence  $l+1$  is the smallest positive root of the congruences  $a^2x^2 - D \equiv 0 \pmod{p^t}$  and  $a^2x^2 - D \equiv 0 \pmod{p^{t+1}}$ . But  $d_{p^t}$  is equal to the smallest positive root of the congruence  $a^2x^2 - D \equiv 0 \pmod{p^{t+1}}$  if  $p = 2$ , and  $d_{p^t}$  is equal to the smallest positive root of the congruence  $a^2x^2 - D \equiv 0 \pmod{p^t}$  if  $p \neq 2$ . Thus  $d_{p^t} = l+1$ . However,  $k \leq l$  since  $k \in \mathcal{K}_f$ . So we obtain that  $d_{p^t} > k$  as desired.

The proof of Lemma 2.12 is complete.  $\square$

**Lemma 2.13.** *Let  $\mathcal{K}_f$  be nonempty.*

(i). *Let  $a$  be odd and  $D_4 \equiv 1 \pmod{8}$ . If  $k \in \mathcal{K}_f$  and there is an integer  $e > v_2(D)$  such that  $d_{2^e} \leq k < d_{2^{e+1}}$ , then we have*

$$\max_{1 \leq i \leq k} \{v_2(a^2 i^2 - D)\} = v_2(a^2 d_{2^e}^2 - D) = e + 1.$$

(ii). *Let  $p$  be an odd prime with  $p \nmid a$ . For any  $k \in \mathcal{K}_f$  such that  $d_{p^e} \leq k < d_{p^{e+1}}$  for some nonnegative integer  $e$ , we have*

$$\max_{1 \leq i \leq k} \{v_p(a^2 i^2 - D)\} = v_p(a^2 d_{p^e}^2 - D) = e.$$

*Proof.* (i). By Lemma 2.9 (iii),  $d_{2^e}$  is the smallest solution of  $a^2 x^2 - D \equiv 0 \pmod{2^{e+1}}$ . Since  $k \geq d_{2^e}$ , we have

$$\max_{1 \leq i \leq k} \{v_2(a^2 i^2 - D)\} \geq v_2(a^2 d_{2^e}^2 - D) \geq e + 1.$$

Part (iii) of Lemma 2.9 also tells us that  $d_{2^{e+1}}$  is the smallest positive solution of  $a^2 x^2 - D \equiv 0 \pmod{2^{e+2}}$ . Thus  $v_2(a^2 i^2 - D) < e + 2$  for all  $1 \leq i < d_{2^{e+1}}$ . It then follows immediately from  $k < d_{2^{e+1}}$  that

$$\max_{1 \leq i \leq k} \{v_2(a^2 i^2 - D)\} \leq e + 1.$$

Therefore we obtain the desired result  $\max_{1 \leq i \leq k} \{v_2(a^2 i^2 - D)\} = v_2(a^2 d_{2^e}^2 - D) = e + 1$ . Part (i) is proved.

(ii). Since  $k \geq d_{p^e}$ ,  $d_{p^e} < \infty$ . By parts (i) and (iii) of Lemma 2.10, we derive that

$$e \leq v_p(a^2 d_{p^e}^2 - D) \leq \max_{1 \leq i \leq k} \{v_p(a^2 i^2 - D)\}.$$

Noticing the facts that  $k < d_{p^{e+1}}$  and  $d_{p^{e+1}}$  is the smallest solution of  $a^2 x^2 - D \equiv 0 \pmod{p^{e+1}}$ , we obtain  $\max_{1 \leq i \leq k} \{v_p(a^2 i^2 - D)\} \leq e$ . It then follows that

$$\max_{1 \leq i \leq k} \{v_p(a^2 i^2 - D)\} = v_p(a^2 d_{p^e}^2 - D) = e$$

as required. Part (ii) is true. So Lemma 2.13 is proved.  $\square$

### 3. A characterization on $f$ such that $g_{k,f}$ can be extended to a periodic arithmetic function

In this section, we first characterize all the quadratic primitive polynomials  $f$  with integer coefficients such that  $g_{k,f}$  can be extended to a periodic arithmetic function. Subsequently, we transfer the smallest period problem into a local analysis problem.

**Theorem 3.1.** *Let  $k$  be a positive integer. The function  $g_{k,f}$  can be extended to a periodic arithmetic function if and only if  $\mathcal{K}_f$  is nonempty and  $k \in \mathcal{K}_f$ . Furthermore, if  $g_{k,f}$  can be extended to a periodic arithmetic function, then  $B_k$  is its period.*

*Proof.* First we show the necessity part. Let  $g_{k,f}$  can be extended to a periodic arithmetic function. Suppose that either  $\mathcal{K}_f$  is empty, or  $\mathcal{K}_f$  is nonempty and  $k \notin \mathcal{K}_f$ . Then  $D$  is a square of the form  $a^2 i_0^2$  for some  $i_0$  with  $1 \leq i_0 \leq k$ , which implies that  $f(x)$  is reducible. We may let

$$f(x) = ax^2 + bx + c := (a_1x + b_1)(a_2x + b_2)$$

with  $\gcd(a_1, b_1) = \gcd(a_2, b_2) = 1$  and  $a_1, a_2 \in \mathbb{N}^*$ . Then

$$D = (a_2b_1 - a_1b_2)^2 = a_1^2 a_2^2 i_0^2.$$



In other words, we have  $a_2b_1 - a_1b_2 = \pm a_1a_2i_0$  and so  $a_2(b_1 \pm a_1i_0) = a_1b_2$ . It follows that  $a_1 = a_2$  and  $b_2 = b_1 \pm a_1i_0$ . So we can write  $f$  as

$$f(x) = (a_1x + b_1)(a_1x + b_1 \pm a_1i_0).$$

If  $b_2 = b_1 + a_1i_0$ , then for any positive integer  $n$ ,  $a_1n + b_1 + a_1i_0$  divides

$$\frac{|f(n)f(n+i_0)|}{\text{lcm}(f(n), f(n+i_0))}.$$

Hence  $(a_1n + b_1 + a_1i_0) \mid g_{k,f}(n)$  which implies that  $g_{k,f}(n) \geq a_1n + b_1 + a_1i_0$ .

If  $b_2 = b_1 - a_1i_0$ , we obtain that  $(a_1n + b_1) \mid g_{k,f}(n)$  and  $g_{k,f}(n) \geq a_1n + b_1$ . Thus  $g_{k,f}(n)$  tends to infinity as  $n$  tends to infinity. This is impossible since  $g_{k,f}$  can be extended to an integer-valued periodic arithmetic function implies that  $g_{k,f}(n)$  is bounded.

Consequently, we show the sufficiency part. Let  $\mathcal{K}_f$  be nonempty and  $k \in \mathcal{K}_f$ . Then we have  $B_k = \text{lcm}_{1 \leq i \leq k} \{i(a^2i^2 - D)\} \neq 0$ . For any given positive integer  $n \in \mathbb{N}^* \setminus Z_{k,f}$ , we derive from the identity

$$(2an + 3aj - ai + b)f(n+i) - (2an + 3ai - aj + b)f(n+j) = (j-i)(a^2(j-i)^2 - D)$$

that

$$\gcd(f(n+i), f(n+j)) \mid \text{lcm}_{0 \leq i < j \leq k} \{(j-i)(a^2(j-i)^2 - D)\} = B_k. \quad (3.1)$$

We then obtain that

$$\gcd(f(n+i), f(n+j)) \mid f(n+i \pm B_k) \text{ and } \gcd(f(n+i), f(n+j)) \mid f(n+j \pm B_k).$$

It infers that

$$\gcd(f(n+i), f(n+j)) \mid \gcd(f(n+B_k+i), f(n+B_k+j))$$

and

$$\gcd(f(n+i), f(n+j)) \mid \gcd(f(n-B_k+i), f(n-B_k+j)). \quad (3.2)$$

Replacing  $n$  by  $n + B_k$  in (3.2), one gets

$$\gcd(f(n+B_k+i), f(n+B_k+j)) \mid \gcd(f(n+i), f(n+j)).$$

Therefore

$$\gcd(f(n+i), f(n+j)) = \gcd(f(n+i+B_k), f(n+j+B_k))$$

for any positive integer  $n \in \mathbb{N}^* \setminus Z_{k,f}$  and any integers  $i, j$  with  $0 \leq i < j \leq k$ . But Theorem 7.3 in Chapter 1 of [19] (see Page 11 of [19]) tells us that

$$g_{k,f}(n) = \prod_{r=1}^k \prod_{0 \leq i_0 < \dots < i_r \leq k} (\gcd(f(n+i_0), \dots, f(n+i_r)))^{(-1)^{r-1}}$$

and

$$g_{k,f}(n+B_k) = \prod_{r=1}^k \prod_{0 \leq i_0 < \dots < i_r \leq k} (\gcd(f(n+B_k+i_0), \dots, f(n+B_k+i_r)))^{(-1)^{r-1}}.$$

Thus  $g_{k,f}(n+B_k) = g_{k,f}(n)$  for any positive integer  $n \in \mathbb{N}^* \setminus Z_{k,f}$ , and  $g_{k,f}$  is periodic with  $B_k$  as its period. Evidently, if  $Z_{k,f}$  is empty, then  $g_{k,f}$  is a periodic arithmetic function. Obviously,  $g_{k,f}$  is a periodic arithmetic function if  $f$  is irreducible since  $Z_{k,f}$  is empty for irreducible polynomials  $f$ . Only when  $f$  is reducible,  $Z_{k,f}$  is not empty. In this case, for all  $n \in Z_{k,f}$ , we can always find a positive integer  $a_0$  such that  $n + a_0B_k \in \mathbb{N}^* \setminus Z_{k,f}$ . By defining  $g_{k,f}(n) := g_{k,f}(n + a_0B_k)$  for each  $n \in Z_{k,f}$ , we get the extended periodic arithmetic function  $g_{k,f} : \mathbb{N}^* \rightarrow \mathbb{N}^*$  with  $B_k$  as its period.  $\square$

After giving a characterization on  $f$  so that  $g_{k,f}$  can be extended to a periodic arithmetic function, we now turn our attention to determining the smallest period of  $g_{k,f}$ . Our basic idea is to transfer the problem to a local analysis problem such that we can provide local analysis to  $g_{k,f}$ . In what follows, when mentioning  $g_{k,f}$ , we will mean the extended periodic arithmetic function  $g_{k,f}$ . For any given prime  $p$ , we define the arithmetic function  $g_{p,k,f}$  for any positive integer  $n$  by  $g_{p,k,f}(n) := v_p(g_{k,f}(n))$ . If  $g_{k,f}$  is periodic with  $P_{k,f}$  as its smallest period, then  $g_{p,k,f}$  is periodic and  $P_{k,f}$  is a period of  $g_{p,k,f}$ . Let  $P_{p,k,f}$  be the smallest period of  $g_{p,k,f}$ . Then  $P_{p,k,f} | P_{k,f}$ . The following result factors the global period  $P_{k,f}$  into the product of the local periods  $P_{p,k,f}$ .

**Lemma 3.2.** *For any prime  $p$ ,  $P_{p,k,f}$  divides  $p^{v_p(B_k)}$ . Further, we have*

$$P_{k,f} = \prod_{p|B_k} P_{p,k,f}.$$

*Proof.* For any positive integer  $n$  and any two integers  $i, j$  with  $0 \leq i < j \leq k$ , we get by (3.1) that

$$v_p(\gcd(f(n+i), f(n+j))) = \min\{v_p(f(n+i)), v_p(f(n+j))\} \leq v_p(B_k),$$

which means that  $v_p(f(n+i)) \leq v_p(B_k)$  or  $v_p(f(n+j)) \leq v_p(B_k)$ . Therefore

$$v_p(f(n+i)) \leq v_p(f(n+i \pm p^{v_p(B_k)}))$$

or

$$v_p(f(n+j)) \leq v_p(f(n+j \pm p^{v_p(B_k)})).$$

Hence we derive that

$$\begin{aligned} v_p(\gcd(f(n+i), f(n+j))) &\leq \min(v_p(f(n+i + p^{v_p(B_k)})), v_p(f(n+j + p^{v_p(B_k)}))) \\ &= v_p(\gcd(f(n+i + p^{v_p(B_k)}), f(n+j + p^{v_p(B_k)}))) \end{aligned}$$

and

$$v_p(\gcd(f(n+i), f(n+j))) \leq v_p(\gcd(f(n+i - p^{v_p(B_k)}), f(n+j - p^{v_p(B_k)}))). \quad (3.3)$$

Replacing  $n$  by  $n + p^{v_p(B_k)}$  in (3.3), we obtain

$$v_p(\gcd(f(n+i + p^{v_p(B_k)}), f(n+j + p^{v_p(B_k)}))) \leq v_p(\gcd(f(n+i), f(n+j))).$$

Thus we have that

$$v_p(\gcd(f(n+i + p^{v_p(B_k)}), f(n+j + p^{v_p(B_k)}))) = v_p(\gcd(f(n+i), f(n+j)))$$

for any positive integer  $n$  and any two integers  $0 \leq i < j \leq k$ . It then follows from Theorem 7.3 in Chapter 1 of [19] that  $g_{p,k,f}(n) = g_{p,k,f}(n + p^{v_p(B_k)})$  for any positive integer  $n$ . Hence we get that  $p^{v_p(B_k)}$  is a period of  $g_{p,k,f}$  and thus  $P_{p,k,f} | p^{v_p(B_k)}$ . It tells us that  $P_{p,k,f}$  are relatively prime for different prime numbers  $p$  and  $P_{p,k,f} = 1$  for all primes  $p \nmid B_k$ .

On the other hand, since  $P_{q,k,f} | P_{k,f}$  for each prime  $q$ , we have

$$\prod_{\text{prime } q|B_k} P_{q,k,f} \mid P_{k,f}.$$

Since  $P_{q,k,f} = 1$  for all primes  $q \nmid B_k$ , we have for each prime  $p$  and any positive integer  $n$  that

$$v_p(g_{k,f}(n + \prod_{\text{prime } q|B_k} P_{q,k,f})) = v_p(g_{k,f}(n)),$$

which implies that  $\prod_{p|B_k} P_{p,k,f}$  is a period of  $g_{k,f}$  and

$$P_{k,f} \left| \prod_{p|B_k} P_{p,k,f} \right.$$

Thus the desired result follows immediately. The proof of Lemma 3.2 is complete.  $\square$

By Lemma 3.2, to get the global period  $P_{k,f}$ , it is sufficient to determine the exact value of the local period  $P_{p,k,f}$  for all the primes  $p|B_k$ .

#### 4. $p$ -Adic analysis of $g_{k,f}$ and determination of local periods

In this section, we supply detailed local analysis to all extended periodic arithmetic functions  $g_{k,f}$  presented in Section 3. Let

$$S_{k,f}(n) := \{f(n), f(n+1), \dots, f(n+k)\}$$

for any positive integer  $n$ . By the definition of  $d_{p^{e+1}}$ , we know that if  $e$  is a nonnegative integer such that  $d_{p^e} \leq k < d_{p^{e+1}}$ , then there is at most one term divisible by  $p^{e+1}$  in the set  $S_{k,f}(n)$  for any positive integer  $n$ . We have

$$\begin{aligned} g_{p,k,f}(n) &= \sum_{m \in S_{k,f}(n)} v_p(m) - \max_{m \in S_{k,f}(n)} \{v_p(m)\} \\ &= \sum_{i=1}^{\infty} \#\{m \in S_{k,f}(n) : v_p(m) \geq i\} - \sum_{i=1}^{\infty} (1 \text{ if } v_p(m) \geq i \text{ for some } m \in S_{k,f}(n)) \\ &= \sum_{i=1}^{\infty} \#\{m \in S_{k,f}(n) : p^i \mid m\} - \sum_{i=1}^{\infty} (1 \text{ if } p^i \text{ divides some } m \in S_{k,f}(n)) \\ &= \sum_{i=1}^{\infty} h_{p,i}(n), \end{aligned} \tag{4.1}$$

where  $h_{p,i}(n) := \max(0, \#\{m \in S_{k,f}(n) : p^i \mid m\} - 1)$ . It follows that if the set  $\{m \in S_{k,f}(n) : p^i \mid m\}$  is nonempty, then

$$h_{p,i}(n) := \#\{m \in S_{k,f}(n) : p^i \mid m\} - 1.$$

**Lemma 4.1.** *Let  $\mathcal{K}_f$  be nonempty and  $p$  be a prime with  $p \nmid a$ . Let  $k \in \mathcal{K}_f$  and  $e$  be the positive integer such that  $d_{p^e} \leq k < d_{p^{e+1}}$ . If  $e \leq v_p(D)$ , then there is a positive integer  $n_0$  such that  $g_{p,k,f}(n_0 + p^{\lceil e/2 \rceil - 1}) \neq g_{p,k,f}(n_0)$ .*

*Proof.* Let first  $n$  be any positive integer and  $e \leq v_p(D)$ . Consider the difference

$$\Delta_1(n) := g_{p,k,f}(n + p^{\lceil e/2 \rceil - 1}) - g_{p,k,f}(n).$$

Then to show Lemma 4.1, it suffices to find some suitable integer  $n$  such that  $\Delta_1(n) \neq 0$ , which will be done in the following.

For any integer  $i \geq e + 1$ , since  $d_{p^e} \leq k < d_{p^{e+1}}$ , there is at most one term divisible by  $p^i$  in the set  $S_{k,f}(n)$  for any positive integer  $n$ . Thus  $\#\{m \in S_{k,f}(n) : p^i \mid f(m)\} \leq 1$  and so  $h_{p,i}(n) = 0$  for any positive integer  $n$ . It follows from (4.1) that

$$\Delta_1(n) = \sum_{i=1}^e (h_{p,i}(n + p^{\lceil e/2 \rceil - 1}) - h_{p,i}(n)). \tag{4.2}$$

We claim that for any integers  $m$  and  $i$  with  $1 \leq i \leq e$ , we have

$$v_p(f(n)) \geq i \iff v_p(f(n + mp^{\lceil e/2 \rceil})) \geq i. \quad (4.3)$$

For the case  $p = 2$  and  $2 \nmid a$ , since  $v_2(D) \geq e \geq 1$ , we have that  $v_2(D) \geq 2$  and  $b$  is even. If  $v_2(f(n)) \geq i$ , then

$$\left(an + \frac{b}{2}\right)^2 \equiv \frac{D}{4} \pmod{2^i}.$$

It follows that  $v_2(an + \frac{b}{2}) \geq \lceil \frac{i}{2} \rceil$  if  $i \leq v_2(D) - 2$ , and  $v_2(an + \frac{b}{2}) = \lceil \frac{i}{2} \rceil - 1$  if  $i = v_2(D) - 1$  or  $v_2(D)$ . Hence for any integer  $m$ , we obtain

$$\begin{aligned} v_2(f(n + m2^{\lceil e/2 \rceil})) &= v_2(f(n) + (an + \frac{b}{2})m2^{\lceil e/2 \rceil+1} + am^2 \cdot 2^{2\lceil e/2 \rceil}) \\ &\geq \min \left\{ i, \left\lceil \frac{i}{2} \right\rceil - 1 + \left\lceil \frac{e}{2} \right\rceil + 1 + v_2(m), 2\left\lceil \frac{e}{2} \right\rceil + 2v_2(m) \right\} \geq i. \end{aligned}$$

Similarly, one has

$$v_2(f(n - m2^{\lceil e/2 \rceil})) \geq i. \quad (4.4)$$

Conversely, if  $v_2(f(n + m2^{\lceil e/2 \rceil})) \geq i$ , then we obtain by replacing  $n$  with  $n + m2^{\lceil e/2 \rceil}$  in (4.4) that  $v_2(f(n)) \geq i$ . Therefore for any integers  $m$  and  $i$  with  $1 \leq i \leq e$ , we have

$$v_2(f(n)) \geq i \iff v_2(f(n + m2^{\lceil e/2 \rceil})) \geq i. \quad (4.5)$$

That is, the claim is true for the case  $p = 2$  and  $2 \nmid a$ .

For the case  $p \neq 2$  and  $p \nmid a$ , if  $v_p(f(n)) \geq i$ , then it follows from  $e \leq v_p(D)$  and  $(2an + b)^2 \equiv D \pmod{p^i}$  that  $v_p(2an + b) \geq \lceil i/2 \rceil$ , which implies that

$$v_p(f(n \pm mp^{\lceil e/2 \rceil})) \geq \min \{ i, \lceil i/2 \rceil + \lceil e/2 \rceil + v_p(m), 2\lceil e/2 \rceil + 2v_p(m) \} \geq i. \quad (4.6)$$

If  $v_p(f(n + mp^{\lceil e/2 \rceil})) \geq i$ , replacing  $n$  with  $n + mp^{\lceil e/2 \rceil}$  in (4.6), then we get that  $v_p(f(n)) = v_p(f(n + mp^{\lceil e/2 \rceil} - mp^{\lceil e/2 \rceil})) \geq i$ . Hence (4.3) holds in this case. The claim is proved.

Replacing  $e$  by  $2\lceil e/2 \rceil - 2$ , then (4.3) gives that for any given  $1 \leq i \leq 2\lceil e/2 \rceil - 2$  and any  $0 \leq j \leq k$ ,

$$v_p(f(n + j)) \geq i \iff v_p(f(n + j + p^{\lceil e/2 \rceil - 1})) \geq i.$$

Thus the number of terms divisible by  $p^i$  in  $S_{k,f}(n)$  is equal to that in  $S_{k,f}(n + p^{\lceil e/2 \rceil - 1})$  for each  $1 \leq i \leq 2\lceil e/2 \rceil - 2$ . It implies that

$$h_{p,i}(n + p^{\lceil e/2 \rceil - 1}) = h_{p,i}(n)$$

for each  $1 \leq i \leq 2\lceil e/2 \rceil - 2$ . Therefore by (4.2), we derive that

$$\Delta_1(n) = \sum_{i=2\lceil e/2 \rceil - 1}^e (h_{p,i}(n + p^{\lceil e/2 \rceil - 1}) - h_{p,i}(n)). \quad (4.7)$$

Since  $k \geq d_{p^e}$  implying that  $d_{p^e} < \infty$ , by the definition of  $d_{p^e}$  we know that  $S(f, p^e)$  is nonempty. Define

$$x_0 := \text{the smallest positive solution of the congruence } f(x) \equiv 0 \pmod{p^e}.$$

Then by Lemma 2.2 (i)-(ii) and Lemma 2.3 (i), any term divisible by  $p^e$  in the quadratic sequence  $\{f(m)\}_{m=1}^\infty$  must be of the form  $f(x_0 + tp^{\lceil e/2 \rceil})$  with  $t \in \mathbb{N}$ . But  $\lceil e/2 \rceil = \lceil (e-1)/2 \rceil$  if  $e$  is even. Thus by Lemma 2.2 (i)-(ii) and Lemma 2.3 (i), the terms divisible by  $p^{e-1}$  are exactly the terms divisible by  $p^e$  in the quadratic progression  $\{f(m)\}_{m=1}^\infty$ .

Hence the terms divisible by  $p^{e-1}$  are exactly the terms divisible by  $p^e$  in the set  $S_{k,f}(n)$  (resp.  $S_{k,f}(n + p^{\lceil e/2 \rceil - 1})$ ) if  $e$  is even. Namely,

$$\{\bar{m} \in S_{k,f}(m) : p^{e-1} \mid \bar{m}\} = \{\bar{m} \in S_{k,f}(m) : p^e \mid \bar{m}\}$$

for  $m = n, n + p^{\lceil e/2 \rceil - 1}$ . So  $h_{p,e-1}(m) = h_{p,e}(m)$  for  $m = n, n + p^{\lceil e/2 \rceil - 1}$ , which implies that

$$h_{p,e-1}(n + p^{\lceil e/2 \rceil - 1}) - h_{p,e-1}(n) = h_{p,e}(n + p^{\lceil e/2 \rceil - 1}) - h_{p,e}(n)$$

if  $e$  is even. It then follows from (4.7) that

$$\Delta_1(n) = 2^{\frac{1+(-1)^e}{2}} (h_{p,e}(n + p^{\lceil e/2 \rceil - 1}) - h_{p,e}(n)). \quad (4.8)$$

Since the terms divisible by  $p^e$  in the sets  $S_{k,f}(n)$  and  $S_{k,f}(n + p^{\lceil e/2 \rceil - 1})$  are of the form  $f(x_0 + tp^{\lceil e/2 \rceil})$  with  $t \in \mathbb{N}$ , in order to compute  $\Delta_1(n)$ , it is sufficient to compare the number of terms of the form  $f(x_0 + tp^{\lceil e/2 \rceil})$  ( $t \in \mathbb{N}$ ) in the set  $S_{k,f}(n)$  with that in the set  $S_{k,f}(n + p^{\lceil e/2 \rceil - 1})$ . By Lemma 2.9 (i) and Lemma 2.10 (i),  $d_{p^e} = p^{\lceil e/2 \rceil}$ . But  $k \geq d_{p^e}$ . Thus  $k \geq p^{\lceil e/2 \rceil}$ . Since  $v_p(k+1) < \lceil e/2 \rceil$ , we can suppose that

$$k = k_0 p^{\lceil e/2 \rceil} + r$$

for unique two integers  $k_0$  and  $r$  with  $k_0 \geq 1$  and  $0 \leq r \leq p^{\lceil e/2 \rceil} - 2$ .

If  $0 \leq r < p^{\lceil e/2 \rceil} - p^{\lceil e/2 \rceil - 1}$ , then  $p^{\lceil e/2 \rceil - 1} \leq r + p^{\lceil e/2 \rceil - 1} < p^{\lceil e/2 \rceil}$ . Hence the number of integers  $t$  such that

$$x_0 + p^{\lceil e/2 \rceil - 1} \leq x_0 + tp^{\lceil e/2 \rceil} \leq x_0 + k + p^{\lceil e/2 \rceil - 1}$$

is equal to

$$\left\lfloor \frac{k + p^{\lceil e/2 \rceil - 1}}{p^{\lceil e/2 \rceil}} \right\rfloor = k_0 + \left\lfloor \frac{r + p^{\lceil e/2 \rceil - 1}}{p^{\lceil e/2 \rceil}} \right\rfloor = k_0.$$

So there are exactly  $k_0$  terms divisible by  $p^e$  in the set  $S_{k,f}(x_0 + p^{\lceil e/2 \rceil - 1})$ . Thus  $h_{p,e}(x_0 + p^{\lceil e/2 \rceil - 1}) = k_0 - 1$ . Similarly, by counting the number of integers  $t$  satisfying  $x_0 \leq x_0 + tp^{\lceil e/2 \rceil} \leq x_0 + k$ , we get that the number of terms divisible by  $p^e$  in  $S_{k,f}(x_0)$  equals  $\left\lfloor \frac{k}{p^{\lceil e/2 \rceil}} \right\rfloor + 1 = k_0 + 1$  and so  $h_{p,e}(x_0) = k_0$ . Thus we derive from (4.8) that

$$\Delta_1(x_0) = -2^{\frac{1+(-1)^e}{2}}. \quad (4.9)$$

If  $p^{\lceil e/2 \rceil} - p^{\lceil e/2 \rceil - 1} \leq r \leq p^{\lceil e/2 \rceil} - 2$ , then we have

$$p^{\lceil e/2 \rceil} - p^{\lceil e/2 \rceil - 1} + 1 \leq r + 1 \leq p^{\lceil e/2 \rceil} - 1$$

and

$$p^{\lceil e/2 \rceil} + 1 \leq r + p^{\lceil e/2 \rceil - 1} + 1 \leq p^{\lceil e/2 \rceil} + p^{\lceil e/2 \rceil - 1} - 1.$$

Therefore, by counting the number of integers  $t$  such that  $x_0 + 1 \leq x_0 + tp^{\lceil e/2 \rceil} \leq x_0 + k + 1$  (resp.  $x_0 + p^{\lceil e/2 \rceil - 1} + 1 \leq x_0 + tp^{\lceil e/2 \rceil} \leq x_0 + p^{\lceil e/2 \rceil - 1} + k + 1$ ), we deduce that

$$h_{p,e}(x_0 + 1) = \left\lfloor \frac{k+1}{p^{\lceil e/2 \rceil}} \right\rfloor - 1 = k_0 + \left\lfloor \frac{r+1}{p^{\lceil e/2 \rceil}} \right\rfloor - 1 = k_0 - 1$$

and

$$h_{p,e}(x_0 + p^{\lceil e/2 \rceil - 1} + 1) = \left\lfloor \frac{k + p^{\lceil e/2 \rceil - 1} + 1}{p^{\lceil e/2 \rceil}} \right\rfloor - 1 = k_0 + \left\lfloor \frac{r + p^{\lceil e/2 \rceil - 1} + 1}{p^{\lceil e/2 \rceil}} \right\rfloor - 1 = k_0$$

It then follows from (4.8) that

$$\Delta_1(x_0 + 1) = 2^{\frac{1+(-1)^e}{2}}. \quad (4.10)$$

Thus the desired result follows immediately from (4.9) and (4.10). This completes the proof of Lemma 4.1.  $\square$

With the help of (4.1), we can make a detailed local analysis to determine the local period  $P_{p,k,f}$  for each prime factor  $p$  of  $B_k$ . We have the following results.

**Lemma 4.2.** *Let  $p$  be a prime such that  $p|a$ . Then*

$$P_{p,k,f} = \begin{cases} p^{v_p(B_k)}, & \text{if } p \nmid b \text{ and } v_p(k+1) < v_p(B_k), \\ 1, & \text{otherwise.} \end{cases}$$

*Proof.* If  $p|b$ , then  $p \nmid f(n)$  for any positive integer  $n$  since  $\gcd(a, b, c) = 1$ . In other words,  $g_{p,k,f}(n) = 0$  for any positive integer  $n$ . Thus  $P_{p,k,f} = 1$  as required. Lemma 4.2 is true if  $p|b$ .

Now we let  $p \nmid b$ . Then  $p \nmid D = b^2 - 4ac$  since  $p|a$ . It follows that  $v_p(a^2n^2 - D) = 0$  for any positive integer  $n$ . Hence

$$v_p(B_k) = v_p(\text{lcm}_{1 \leq i \leq k} \{i(a^2i^2 - D)\}) = \max_{1 \leq i \leq k} \{v_p(i)\} = v_p(L_k).$$

By Lemma 2.1, there is exactly one term divisible by  $p^e$  in any consecutive  $p^e$  terms of the quadratic progression  $\{f(n+m)\}_{m \in \mathbb{N}}$  for any given positive integers  $e$  and  $n$ . Since  $p^{v_p(L_k)} \leq k < p^{v_p(L_k)+1}$ , it follows from Lemma 2.8 that

$$d_{p^{v_p(L_k)}} \leq k < d_{p^{v_p(L_k)+1}}.$$

Then there is at most one term divisible by  $p^{v_p(L_k)+1}$  in  $S_{k,f}(n)$  for any positive integer  $n$ . Consider the following two cases.

**Case 1.**  $v_p(k+1) \geq v_p(B_k) = v_p(L_k)$ . By Lemma 2.1, we deduce that there are exactly  $\frac{k+1}{p^e}$  terms divisible by  $p^e$  in  $S_{k,f}(n)$  (resp.  $S_{k,f}(n+1)$ ) for any positive integer  $n$  and each  $e \in \{1, \dots, v_p(L_k)\}$ . On the other hand, since there is at most one term divisible by  $p^{v_p(L_k)+1}$  in  $S_{k,f}(n)$  (resp.  $S_{k,f}(n+1)$ ), we have by (4.1) that

$$g_{p,k,f}(n) = \sum_{e=1}^{v_p(L_k)} \left( \frac{k+1}{p^e} - 1 \right) = g_{p,k,f}(n+1)$$

for any positive integer  $n$ . Therefore  $P_{p,k,f} = 1$  as desired. Lemma 4.2 is proved in this case.

**Case 2.**  $v_p(k+1) < v_p(B_k) = v_p(L_k)$ . Evidently,  $v_p(L_k) \geq 1$ . Since there is at most one term divisible by  $p^{v_p(L_k)+1}$  in  $S_{k,f}(n)$  for any positive integer  $n$ , we have  $h_{p,e}(n) = 0$  if  $e \geq v_p(L_k) + 1$ . Thus we can deduce from (4.1) that

$$g_{p,k,f}(n) = \sum_{e=1}^{v_p(L_k)} h_{p,e}(n).$$

By Lemma 3.2,  $p^{v_p(L_k)}$  is a period of  $g_{p,k,f}$ . So it remains to prove that  $p^{v_p(L_k)-1}$  is not a period of  $g_{p,k,f}$ . For any integer  $e$  such that  $1 \leq e \leq v_p(L_k)-1$ , since  $f(n+p^{v_p(L_k)-1}) \equiv f(n) \pmod{p^e}$  for any positive integer  $n$ ,  $p^{v_p(L_k)-1}$  is a period of  $h_{p,e}$ . Hence we only need to prove that  $p^{v_p(L_k)-1}$  is not a period of  $h_{p,v_p(L_k)}$ . Since  $v_p(k+1) < v_p(L_k)$ , we can pick an  $r \in \{0, 1, \dots, p^{v_p(L_k)} - 2\}$  such that  $k \equiv r \pmod{p^{v_p(L_k)}}$ .

**Subcase 2.1.**  $0 \leq r < p^{v_p(L_k)} - p^{v_p(L_k)-1}$ . Then by Lemma 2.1, we can choose a positive integer  $n_0$  such that  $f(n_0) \equiv 0 \pmod{p^{v_p(L_k)}}$ . And so the terms divisible by

$p^{v_p(L_k)}$  in the quadratic sequence  $\{f(n_0 + i)\}_{i \in \mathbb{N}}$  must be of the form  $f(n_0 + tp^{v_p(L_k)})$  for some  $t \in \mathbb{N}$ . It then follows that there are exactly  $1 + \left\lfloor \frac{k}{p^{v_p(L_k)}} \right\rfloor$  terms divisible by  $p^{v_p(L_k)}$  in  $S_{k,f}(n_0)$  and there are exactly

$$\left\lfloor \frac{k + p^{v_p(L_k)-1}}{p^{v_p(L_k)}} \right\rfloor = \left\lfloor \frac{k-r}{p^{v_p(L_k)}} \right\rfloor + \left\lfloor \frac{p^{v_p(L_k)-1} + r}{p^{v_p(L_k)}} \right\rfloor = \left\lfloor \frac{k}{p^{v_p(L_k)}} \right\rfloor$$

terms divisible by  $p^{v_p(L_k)}$  in  $S_{k,f}(n_0 + p^{v_p(L_k)-1})$ , where the last equality is derived from  $k \equiv r \pmod{p^{v_p(L_k)}}$  and  $0 \leq r < p^{v_p(L_k)} - p^{v_p(L_k)-1}$ . Thus

$$h_{p,v_p(L_k)}(n_0) = \left\lfloor \frac{k}{p^{v_p(L_k)}} \right\rfloor = h_{p,v_p(L_k)}(n_0 + p^{v_p(L_k)-1}) + 1.$$

That is,  $p^{v_p(L_k)-1}$  is not a period of  $h_{p,v_p(L_k)}$ .

**Subcase 2.2.**  $p^{v_p(L_k)} - p^{v_p(L_k)-1} \leq r \leq p^{v_p(L_k)} - 2$ . Again by Lemma 2.1, we can pick a suitable positive integer  $m_0$  such that

$$f(m_0 + p^{v_p(L_k)-1} - 1) \equiv 0 \pmod{p^{v_p(L_k)}}.$$

It follows that the terms divisible by  $p^{v_p(L_k)}$  in the quadratic sequence  $\{f(m_0 + i)\}_{i \in \mathbb{N}}$  must be of the form  $f(m_0 + p^{v_p(L_k)-1} - 1 + sp^{v_p(L_k)})$  for some  $s \in \mathbb{N}$ . Since  $k \equiv r \pmod{p^{v_p(L_k)}}$  and  $p^{v_p(L_k)} - p^{v_p(L_k)-1} \leq r \leq p^{v_p(L_k)} - 2$ , we can derive that the number of terms divisible by  $p^{v_p(L_k)}$  in the set  $S_{k,f}(m_0)$  is equal to

$$1 + \left\lfloor \frac{k - (p^{v_p(L_k)-1} - 1)}{p^{v_p(L_k)}} \right\rfloor = 1 + \left\lfloor \frac{k}{p^{v_p(L_k)}} \right\rfloor$$

and the number of terms divisible by  $p^{v_p(L_k)}$  in the set  $S_{k,f}(m_0 + p^{v_p(L_k)-1})$  equals

$$\left\lfloor \frac{k+1}{p^{v_p(L_k)}} \right\rfloor = \left\lfloor \frac{k}{p^{v_p(L_k)}} \right\rfloor.$$

Thus

$$h_{p,v_p(L_k)}(m_0) = h_{p,v_p(L_k)}(m_0 + p^{v_p(L_k)-1}) + 1.$$

Namely,  $p^{v_p(L_k)-1}$  is not a period of  $h_{p,v_p(L_k)}$  as required.

The proof of Lemma 4.2 is complete.  $\square$

Now we need only to handle the even prime 2 and the odd prime  $p$  with  $p \nmid a$ , respectively. We first consider the case  $2 \nmid a$ . Since  $D_4 \equiv 1 \pmod{4}$  if  $v_2(D) = 0$ , we have that  $v_2(D) \geq 1$  if  $e = v_2(D)$  with  $D_4 \not\equiv 1 \pmod{4}$ . Therefore, if either  $e = v_2(D)$  with  $D_4 \not\equiv 1 \pmod{4}$  or  $e > v_2(D)$  with  $D_4 \not\equiv 1 \pmod{8}$ , then by Lemma 2.9 (ii),  $d_{2^e} = \infty$ . But there is no integer  $k$  such that  $k \geq d_{2^e}$  for such integers  $e$ . So one only needs to consider the cases occurred exactly in Lemma 4.3.

**Lemma 4.3.** *Let  $a$  be odd and  $\mathcal{K}_f$  be nonempty. Let  $k \in \mathcal{K}_f$  and  $e$  be the nonnegative integer such that  $d_{2^e} \leq k < d_{2^{e+1}}$ . Each of the following is true.*

(i). *If  $e = v_2(D)$  with  $D_4 \equiv 1 \pmod{4}$  or  $e \leq 2\left\lfloor \frac{v_2(D)}{2} \right\rfloor - 1$ , then*

$$P_{2,k,f} = \begin{cases} 2^{\lceil e/2 \rceil}, & \text{if } v_2(k+1) < \lceil e/2 \rceil, \\ 1, & \text{if } v_2(k+1) \geq \lceil e/2 \rceil. \end{cases}$$

(ii). *If  $e > v_2(D)$  with  $D_4 \equiv 1 \pmod{8}$ , then  $P_{2,k,f} = 2^{e - \frac{v_2(D)}{2}}$ .*

*Proof.* Since  $d_{2^e} \leq k < d_{2^{e+1}}$ , there is at most one term divisible by  $2^{e+1}$  in  $S_{k,f}(n)$  for any positive integer  $n$ . It follows from (4.1) that  $2^0 = 1$  is the smallest period of  $g_{2,k,f}$  if  $e = 0$ . So it remains to treat the case  $e \geq 1$ . Let now  $e \geq 1$  and  $n \geq 1$  be an arbitrary given integer. Since  $\#\{m \in S_{k,f}(n) : 2^i \mid m\} \leq 1$  if  $i \geq e + 1$ , then by (4.1),

$$g_{2,k,f}(n) = \sum_{i=1}^e h_{2,i}(n), \quad (4.11)$$

where

$$h_{2,i}(n) = \max(0, \#\{m \in S_{k,f}(n) : 2^i \mid m\} - 1) = \max(0, \#\{0 \leq j \leq k : 2^i \mid f(n+j)\} - 1).$$

Clearly,  $h_{2,i}(n) = \#\{0 \leq j \leq k : 2^i \mid f(n+j)\} - 1$  if there is at least one term divisible by  $2^i$  in  $S_{k,f}(n)$ .

(i). Since  $e = v_2(D) \geq 1$  with  $D_4 \equiv 5 \pmod{8}$  or  $e \leq 2\lfloor \frac{v_2(D)}{2} \rfloor - 1$ , we have  $v_2(D) \geq 2$  and  $b$  is even.

If  $v_2(k+1) \geq \lceil e/2 \rceil$ , comparing  $S_{k,f}(n)$  with  $S_{k,f}(n+1)$ , we find that their distinct terms are  $f(n)$  and  $f(n+k+1)$ . Since  $v_2(k+1) \geq \lceil e/2 \rceil$ , we have  $k+1 = m_0 2^{\lceil e/2 \rceil}$  for some positive integer  $m_0$ . From (4.5), we deduce that for any given integer  $i$  with  $1 \leq i \leq e$ ,  $v_2(f(n)) \geq i$  if and only if  $v_2(f(n+k+1)) \geq i$ . Thus the number of terms divisible by  $2^i$  in  $S_{k,f}(n)$  is equal to the number of terms divisible by  $2^i$  in  $S_{k,f}(n+1)$  for each  $i \in \{1, \dots, e\}$ . Hence by (4.11), we obtain that  $g_{2,k,f}(n) = g_{2,k,f}(n+1)$  for any positive integer  $n$ , which implies that  $P_{2,k,f} = 1$ . Part (i) is true in this case.

In what follows we let  $v_2(k+1) < \lceil e/2 \rceil$ . It follows from (4.5) that for any given  $1 \leq i \leq e$  and for any  $0 \leq j \leq k$ ,

$$v_2(f(n+j)) \geq i \iff v_2(f(n+j+2^{\lceil e/2 \rceil})) \geq i.$$

In other words, the number of terms divisible by  $2^i$  in  $S_{k,f}(n+2^{\lceil e/2 \rceil})$  is equal to the number of terms divisible by  $2^i$  in  $S_{k,f}(n)$  for each  $1 \leq i \leq e$ . So  $g_{2,k,f}(n+2^{\lceil e/2 \rceil}) = g_{2,k,f}(n)$  for any positive integer  $n$ . This infers that  $2^{\lceil e/2 \rceil}$  is a period of  $g_{2,k,f}$ . On the other hand, by Lemma 4.1 one knows that there is a positive integer  $n_0$  such that  $g_{2,k,f}(n_0+2^{\lceil e/2 \rceil-1}) = g_{2,k,f}(n_0)$ . Thus  $2^{\lceil e/2 \rceil-1}$  is not a period of  $g_{2,k,f}$ . Therefore  $2^{\lceil e/2 \rceil}$  is the smallest period of  $g_{2,k,f}$ . Part (i) is proved.

(ii). Since  $D_4$  is odd,  $v_2(D)$  is even. First, we prove that  $2^{e-\frac{v_2(D)}{2}}$  is a period of  $g_{2,k,f}$ . Since  $f(m+2^e) \equiv f(m) \pmod{2^i}$ , we get that  $h_{2,i}(m+2^e) = h_{2,i}(m)$  for any integers  $m$  and  $i$  with  $0 \leq i \leq e$ . So by (4.2),  $g_{2,k,f}(m+2^e) = g_{2,k,f}(m)$  for any integer  $m$ , i.e.,  $2^e = 2^{e-\frac{v_2(D)}{2}}$  is a period of  $g_{2,k,f}$  if  $v_2(D) = 0$ .

Now let  $v_2(D) \geq 2$ . Then  $b$  is even. Let  $l$  be any given positive integer with  $l \geq v_2(D)$ , and let  $i \in \{1, \dots, l\}$  and  $j \in \{0, \dots, k\}$ . If

$$v_2(f(n+j)) \geq i, \quad (4.12)$$

then  $(a(n+j) + \frac{b}{2})^2 \equiv \frac{D}{4} \pmod{2^i}$ , which implies that

$$v_2(a(n+j) + \frac{b}{2}) \geq \min\{\frac{v_2(D)}{2} - 1, \lceil \frac{i}{2} \rceil\}.$$



But  $\min\{\frac{v_2(D)}{2} - 1, \lceil \frac{i}{2} \rceil\} \geq \lceil \frac{i}{2} \rceil$  if  $i \leq v_2(D) - 2$ , and  $\min\{\frac{v_2(D)}{2} - 1, \lceil \frac{i}{2} \rceil\} = \frac{v_2(D)}{2} - 1$  if  $i \geq v_2(D) - 1$ . It then follows that

$$\begin{aligned} v_2(f(n+j+2^{l-\frac{v_2(D)}{2}})) &= v_2\left(f(n+j) + \left(a(n+j) + \frac{b}{2}\right)2^{l-\frac{v_2(D)}{2}+1} + a2^{2l-v_2(D)}\right) \\ &\geq \min\left\{i, l - \frac{v_2(D)}{2} + 1 + \min\left\{\frac{v_2(D)}{2} - 1, \lceil \frac{i}{2} \rceil\right\}, 2l - v_2(D)\right\} \geq i. \end{aligned}$$

Similarly, we have

$$v_2(f(n+j-2^{l-\frac{v_2(D)}{2}})) \geq i. \quad (4.13)$$

If  $v_2(f(n+j+2^{l-\frac{v_2(D)}{2}})) \geq i$ , then the process of (4.13) derived from (4.12) with  $n$  replaced by  $n+2^{l-\frac{v_2(D)}{2}}$  gives us that  $v_2(f(n+j)) \geq i$ . Therefore, if  $l$  is an integer with  $l \geq v_2(D)$ , then for any integers  $i$  and  $j$  with  $1 \leq i \leq l$  and  $0 \leq j \leq k$ , we have

$$v_2(f(n+j)) \geq i \iff v_2(f(n+j+2^{l-\frac{v_2(D)}{2}})) \geq i. \quad (4.14)$$

Since  $e > v_2(D)$ , the number of terms divisible by  $2^i$  in  $S_{k,f}(n+2^{e-\frac{v_2(D)}{2}})$  is equal to the number of terms divisible by  $2^i$  in  $S_{k,f}(n)$  and so  $h_{2,i}(n) = h_{2,i}(n+2^{e-\frac{v_2(D)}{2}})$  for each  $1 \leq i \leq e$ . Thus by (4.11), we have  $g_{2,k,f}(n+2^{e-\frac{v_2(D)}{2}}) = g_{2,k,f}(n)$  for any positive integer  $n$ . So  $2^{e-\frac{v_2(D)}{2}}$  is a period of  $g_{2,k,f}$ .

In the following, we prove that  $2^{e-\frac{v_2(D)}{2}-1}$  is not the period of  $g_{2,k,f}$ . It suffices to  $\Delta_2(n) \neq 0$  for some integer  $n$ , where

$$\Delta_2(n) := g_{2,k,f}(n+2^{e-\frac{v_2(D)}{2}-1}) - g_{2,k,f}(n) = \sum_{i=1}^e (h_{2,i}(n+2^{e-\frac{v_2(D)}{2}-1}) - h_{2,i}(n)). \quad (4.15)$$

Since  $e-1 \geq v_2(D)$ , replacing  $e$  by  $e-1$  in (4.14), one gets that for any integers  $i$  and  $j$  with  $1 \leq i \leq e-1$  and  $0 \leq j \leq k$ ,  $v_2(f(n+j)) \geq i$  if and only if  $v_2(f(n+j+2^{e-\frac{v_2(D)}{2}-1})) \geq i$ . In other words, the number of terms divisible by  $2^i$  in  $S_{k,f}(n)$  is equal to that in  $S_{k,f}(n+2^{e-\frac{v_2(D)}{2}-1})$  for each  $1 \leq i \leq e-1$ . Thus

$$\sum_{i=1}^{e-1} h_{2,i}(n) = \sum_{i=1}^{e-1} h_{2,i}(n+2^{e-\frac{v_2(D)}{2}-1}).$$

It then follows from (4.15) that

$$\Delta_2(n) = h_{2,e}(n+2^{e-\frac{v_2(D)}{2}-1}) - h_{2,e}(n).$$

Therefore, our final task is to find some suitable integer  $n$  such that

$$h_{2,e}(n+2^{e-\frac{v_2(D)}{2}-1}) \neq h_{2,e}(n). \quad (4.16)$$

Since  $a$  is odd and  $D_4 \equiv 1 \pmod{8}$ , we have

$$v_2(a^2(2^{\frac{v_2(D)}{2}})^2 - D) = v_2(D) + v_2(a^2 - D_4) \geq v_2(D) + 3,$$

which means that

$$a^2(2^{\frac{v_2(D)}{2}})^2 - D \equiv 0 \pmod{2^{v_2(D)+3}}.$$

We can easily check that  $2^{\frac{v_2(D)}{2}}$  is the smallest solution of the congruence  $a^2x^2 - D \equiv 0 \pmod{2^i}$  for any  $i$  with  $v_2(D) \leq i \leq v_2(D) + 3$ . Then by parts (i) and (iii) of Lemma 2.8, we derive that

$$d_{2^{v_2(D)-1}} = d_{2^{v_2(D)}} = d_{2^{v_2(D)+1}} = d_{2^{v_2(D)+2}} = 2^{\frac{v_2(D)}{2}}.$$

Since  $d_{2^e} \leq k < d_{2^{e+1}}$  and  $e > v_2(D)$ , we have  $e \geq v_2(D) + 2$ . But  $D_4 \equiv 1 \pmod{8}$ , then by part (iv) of Lemma 2.2,  $S(f, 2^e)$  is nonempty.

We claim that for any  $i \geq e$ ,

$$d_{2^i} < 2^{i - \frac{v_2(D)}{2} - 1}.$$

In fact, by Lemma 2.9 (iii),  $d_{2^i}$  equals the smallest positive solution of  $a^2x^2 - D \equiv 0 \pmod{2^{i+1}}$ . Then  $v_2(d_{2^i}) = \frac{v_2(D)}{2}$ . So  $v_2(a^2(2^{i - \frac{v_2(D)}{2}} - d_{2^i})^2 - D) \geq i + 1$ , and hence  $2^{i - \frac{v_2(D)}{2}} - d_{2^i}$  is also a solution of  $a^2x^2 - D \equiv 0 \pmod{2^{i+1}}$ . From the minimality of  $d_{2^i}$ , we get that  $2^{i - \frac{v_2(D)}{2}} - d_{2^i} \geq d_{2^i}$ . But  $2^{i - \frac{v_2(D)}{2}} - d_{2^i} \neq d_{2^i}$ . Otherwise,

$$v_2(d_{2^i}) = i - \frac{v_2(D)}{2} - 1 \geq v_2(D) + 2 - \frac{v_2(D)}{2} - 1 = \frac{v_2(D)}{2} + 1,$$

which is a contradiction since  $v_2(d_{2^i}) = \frac{v_2(D)}{2}$ . So  $d_{2^i} < 2^{i - \frac{v_2(D)}{2} - 1}$ . The claim is proved. From the claim, we know that

$$d_{2^e} < 2^{e - \frac{v_2(D)}{2} - 1} \text{ and } d_{2^{e+1}} < 2^{e - \frac{v_2(D)}{2}}.$$

Thus we have  $k < d_{2^{e+1}} < 2^{e - \frac{v_2(D)}{2}}$ .

If either  $d_{2^{e+1}} > 2^{e - \frac{v_2(D)}{2} - 1}$  and  $k < 2^{e - \frac{v_2(D)}{2} - 1}$  or  $d_{2^{e+1}} \leq 2^{e - \frac{v_2(D)}{2} - 1}$ , then  $d_{2^e} \leq k < 2^{e - \frac{v_2(D)}{2} - 1}$ . Since  $S(f, 2^e)$  is nonempty, by Lemma 2.6 we can choose a positive integer  $n_0$  such that

$$v_2(f(n_0)) \geq e \text{ and } v_2(f(n_0 + d_{2^e})) \geq e.$$

By Lemma 2.2 (iii), the terms divisible by  $2^e$  in the quadratic progression  $\{f(n_0 + i)\}_{i \in \mathbb{N}}$  must be of the form  $f(n_0 + t_1 2^{e - \frac{v_2(D)}{2}})$  or  $f(n_0 + d_{2^e} + t_2 2^{e - \frac{v_2(D)}{2}})$ , where  $t_1, t_2 \in \mathbb{N}$ . On the one hand, since  $d_{2^e} \leq k < 2^{e - \frac{v_2(D)}{2} - 1}$ ,  $f(n_0)$  and  $f(n_0 + d_{2^e})$  are the only two terms divisible by  $2^e$  in  $S_{k,f}(n_0)$ . On the other hand, since

$$n_0 + d_{2^e} < n_0 + 2^{e - \frac{v_2(D)}{2} - 1} + j \leq n_0 + k + 2^{e - \frac{v_2(D)}{2} - 1} < n_0 + 2^{e - \frac{v_2(D)}{2}}$$

for all  $0 \leq j \leq k$ , there is no term divisible by  $2^e$  in the set  $S_{k,f}(n_0 + 2^{e - \frac{v_2(D)}{2} - 1})$ . It follows that  $h_{2,e}(n_0 + 2^{e - \frac{v_2(D)}{2} - 1}) = 0$  and  $h_{2,e}(n_0) = 1$ . So (4.16) is true in this case.

If  $k \geq 2^{e - \frac{v_2(D)}{2} - 1}$ , then it follows from Lemma 2.6 and the fact that  $S(f, 2^e)$  is nonempty that there is a positive integer  $n_1$  so that

$$v_2(f(n_1 + 2^{e - \frac{v_2(D)}{2} - 1} - 1 - d_{2^e})) \geq e$$

and

$$v_2(f(n_1 + 2^{e - \frac{v_2(D)}{2} - 1} - 1)) \geq e.$$

Hence Lemma 2.2 (iii) tells us that the terms divisible by  $2^e$  in the quadratic progression  $\{f(n_1 + i)\}_{i \in \mathbb{N}}$  should be of the form

$$f(n_1 + 2^{e - \frac{v_2(D)}{2} - 1} - 1 - d_{2^e} + t_1 2^{e - \frac{v_2(D)}{2}}) \quad (4.17)$$

or

$$f(n_1 + 2^{e - \frac{v_2(D)}{2} - 1} - 1 + t_2 2^{e - \frac{v_2(D)}{2}}), \quad (4.18)$$

where  $t_1, t_2 \in \mathbb{N}$ . Since  $k < d_{2^{e+1}}$  and  $d_{2^{e+1}} < 2^{e - \frac{v_2(D)}{2}}$ ,

$$2^{e - \frac{v_2(D)}{2} - 1} \leq j + 2^{e - \frac{v_2(D)}{2} - 1} < 2^{e - \frac{v_2(D)}{2}} + 2^{e - \frac{v_2(D)}{2} - 1} - 1$$

for all  $j \in \{0, 1, \dots, k\}$ . Therefore, there is at most one term of the form (4.17) with  $t_1 \in \mathbb{N}$  and no term of the form (4.18) with  $t_2 \in \mathbb{N}$  in the set  $S_{k,f}(n_1 + 2^{e - \frac{v_2(D)}{2} - 1})$ . Since  $k \geq 2^{e - \frac{v_2(D)}{2} - 1}$  and  $d_{2^e} < 2^{e - \frac{v_2(D)}{2} - 1}$ ,  $f(n_1 + 2^{e - \frac{v_2(D)}{2} - 1} - 1)$  and  $f(n_1 + 2^{e - \frac{v_2(D)}{2} - 1} - 1 - d_{2^e})$  are the only two terms divisible by  $2^e$  in the set  $S_{k,f}(n_1)$ . So  $h_{2,e}(n_1) = 1$  and  $h_{2,e}(n_1 + 2^{e - \frac{v_2(D)}{2}}) = 0$ , which implies that (4.16) holds in the case. This concludes that  $2^{e - \frac{v_2(D)}{2}}$  is the smallest period of  $g_{2,k,f}$ .

The proof of Lemma 4.3 is complete.  $\square$

In what follows, we treat all the odd primes  $p$  with  $p \nmid 2a$  and  $p \mid B_k$ .

**Lemma 4.4.** *Let  $\mathcal{K}_f$  be nonempty and  $p$  be an odd prime with  $p \nmid a$ . Let  $k \in \mathcal{K}_f$  and  $e$  be the nonnegative integer such that  $d_{p^e} \leq k < d_{p^{e+1}}$ . Then*

$$P_{p,k,f} = \begin{cases} 1, & \text{if either } e \leq v_p(D) \text{ and } v_p(k+1) \geq \lceil e/2 \rceil, \\ & \text{or } e > v_p(D) \text{ and } v_p(k+1) \geq e - v_p(D)/2, \\ p^{\lceil e/2 \rceil}, & \text{if } e \leq v_p(D) \text{ and } v_p(k+1) < \lceil e/2 \rceil, \\ p^{e - v_p(D)/2}, & \text{if } e > v_p(D) \text{ and } v_p(k+1) < e - v_p(D)/2. \end{cases}$$

*Proof.* Let  $n \geq 1$  be any positive integer. Since  $d_{p^e} \leq k < d_{p^{e+1}}$ , there is at most one term divisible by  $p^{e+1}$  in the set  $S_{k,f}(n)$  for any positive integer  $n$ . It follows from (4.1) that

$$g_{p,k,f}(n) = \sum_{i=1}^e h_{p,i}(n), \quad (4.19)$$

where

$$h_{p,i}(n) = \#\{0 \leq j \leq k : p^i \mid f(n+j)\} - 1$$

if there is at least term divisible by  $p^i$  in  $S_{k,f}(n)$ . Otherwise,  $h_{p,i}(n) = 0$ . Thus  $g_{p,k,f}(n) = 0$  for any positive integer  $n$ , and so  $P_{p,k,f} = 1$  if  $e = 0$ .

In what follows we let  $e \geq 1$ . Note that if  $e > v_p(D)$  and  $d_{p^e} < \infty$ , then by parts (ii) and (iii) of Lemma 2.10, we know that  $v_p(D)$  is even and  $(D_p/p) = 1$  for such primes  $p$ .

First we show that if  $l \geq v_p(D)$  is an integer, then for any integers  $m$  and  $i$  with  $1 \leq i \leq l$ , we have

$$v_p(f(n)) \geq i \iff v_p(f(n + mp^{l - \frac{v_p(D)}{2}})) \geq i. \quad (4.20)$$

In fact, by (4.3), we know that for any integers  $m$  and  $i$  with  $1 \leq i \leq v_p(D)$ ,

$$v_p(f(n)) \geq i \iff v_p(f(n + mp^{v_p(D)})) \geq i. \quad (4.21)$$

Since  $l \geq v_p(D)$ ,  $p^{l - \frac{v_p(D)}{2}}$  is a multiple of  $p^{\frac{v_p(D)}{2}}$ . Then by (4.21), (4.20) is true for each  $1 \leq i \leq v_p(D)$ . For  $v_p(D) \leq i \leq l$ , we can deduce from  $f(n) \equiv 0 \pmod{p^i}$  that  $v_p(2an + b) \geq v_p(D)/2$ , which implies that

$$v_p(f(n \pm mp^{l - \frac{v_p(D)}{2}})) \geq \min\{i, v_p(D)/2 + l - v_p(D)/2 + v_p(m), 2l - v_p(D) + v_p(m)\} \geq i. \quad (4.22)$$

Conversely, if  $v_p(f(n + mp^{l - \frac{v_p(D)}{2}})) \geq i$ , then replacing  $n$  with  $n + mp^{l - \frac{v_p(D)}{2}}$  in (4.22), we get  $v_p(f(n)) = v_p(f(n + mp^{l - \frac{v_p(D)}{2}} - mp^{l - \frac{v_p(D)}{2}})) \geq i$ . Hence (4.20) is proved.

If either  $e \leq v_p(D)$  and  $v_p(k+1) \geq \lceil e/2 \rceil$ , or  $e > v_p(D)$  and  $v_p(k+1) \geq e - v_p(D)/2$ , then either  $p^{\lceil e/2 \rceil} \mid (k+1)$ , or  $p^{e - v_p(D)/2} \mid (k+1)$ . It then follows immediately from (4.3) and (4.20) with  $l = e$  that for each  $1 \leq i \leq e$ ,  $v_p(f(n)) \geq i$  if and only if  $v_p(f(n+k+1)) \geq$

$i$ . But the distinct terms of the sets  $S_{k,f}(n)$  and  $S_{k,f}(n+1)$  are  $f(n)$  and  $f(n+k+1)$ . Thus the number of terms divisible by  $p^i$  in  $S_{k,f}(n)$  is equal to that in  $S_{k,f}(n+1)$  for any  $i \in \{1, \dots, e\}$ . Thus we have  $h_{p,i}(n+1) = h_{p,i}(n)$  for each  $i \in \{1, \dots, e\}$ , and so by (4.19),  $g_{p,k,f}(n+1) = g_{p,k,f}(n)$  for any positive integer  $n$ . Hence  $P_{p,k,f} = 1$ . So Lemma 4.4 is true if either  $e \leq v_p(D)$  and  $v_p(k+1) \geq \lceil e/2 \rceil$ , or  $e > v_p(D)$  and  $v_p(k+1) \geq e - v_p(D)/2$ .

Now let  $e \leq v_p(D)$  and  $v_p(k+1) < \lceil e/2 \rceil$ . Taking  $m = 1$  in (4.3), we have that for any given  $1 \leq i \leq e$  and for any  $0 \leq j \leq k$ ,  $v_p(f(n+j)) \geq i$  if and only if  $v_p(f(n+j+p^{\lceil e/2 \rceil})) \geq i$ . In other words, the number of terms divisible by  $p^i$  in  $S_{k,f}(n)$  is equal to that in  $S_{k,f}(n+p^{\lceil e/2 \rceil})$  for any  $i \in \{1, \dots, e\}$ . It infers that  $h_{p,i}(n+p^{\lceil e/2 \rceil}) = h_{p,i}(n)$  for each  $i \in \{1, \dots, e\}$ . Thus by (4.19)  $g_{p,k,f}(n+p^{\lceil e/2 \rceil}) = g_{p,k,f}(n)$  for any positive integer  $n$ , and so  $p^{\lceil e/2 \rceil}$  is a period of  $g_{p,k,f}$ . But Lemma 4.1 implies that there is a positive integer  $n_0$  such that  $g_{p,k,f}(n_0+p^{\lceil e/2 \rceil-1}) \neq g_{p,k,f}(n_0)$ . Therefore  $p^{\lceil e/2 \rceil-1}$  is not the period of  $g_{p,k,f}$ . Thus  $p^{\lceil e/2 \rceil}$  is the smallest period of  $g_{p,k,f}$  as required. Thus Lemma 4.4 is true if  $e \leq v_p(D)$  and  $v_p(k+1) < \lceil e/2 \rceil$ .

We only need to deal with the remaining case:  $e > v_p(D)$  and  $v_p(k+1) < e - v_p(D)/2$  which will be done in what follows. First, from (4.20) with  $l = e$  and  $m = 1$ , it follows that for any given  $1 \leq i \leq e$  and for any  $0 \leq j \leq k$ ,  $v_p(f(n+j)) \geq i$  if and only if  $v_p(f(n+j+p^{e-v_p(D)/2})) \geq i$ . Namely, the number of terms divisible by  $p^i$  in  $S_{k,f}(n)$  is equal to that in  $S_{k,f}(n+p^{e-v_p(D)/2})$  for each  $i \in \{1, \dots, e\}$ . Hence  $g_{p,k,f}(n+p^{e-v_p(D)/2}) = g_{p,k,f}(n)$  for any positive integer  $n$  by (4.19). Thus  $p^{e-v_p(D)/2}$  is a period of  $g_{p,k,f}$ .

By Lemma 2.3 (iii), we know that the congruence  $f(x) \equiv 0 \pmod{p^e}$  has exactly two solutions in the interval  $[1, p^{e-\frac{v_p(D)}{2}}]$ . It follows that  $d_{p^e} \leq (p^{e-v_p(D)/2} - 1)/2$ . Therefore, we can find a positive integer  $u_0$  with  $1 \leq u_0 \leq \frac{p+1}{2}$  such that

$$(u_0 - 1)p^{e-v_p(D)/2-1} \leq d_{p^e} < u_0 p^{e-v_p(D)/2-1}.$$

To prove that  $p^{e-v_p(D)/2}$  is the smallest period of  $g_{p,k,f}$ , it suffices to prove that  $u_0 p^{e-\frac{v_p(D)}{2}-1} - 1$  is not a period of  $g_{p,k,f}$ . For this purpose, we define the arithmetic function  $\Delta$  for any positive integer  $n$  by

$$\Delta(n) := g_{p,k,f}(n + u_0 p^{e-v_p(D)/2-1}) - g_{p,k,f}(n). \quad (4.23)$$

Since  $e > v_p(D)$ , we have  $e-1 \geq v_p(D)$ . Picking  $l = e-1$  and  $m = u_0$  in (4.20), we get that for any given  $1 \leq i \leq e-1$  and for any  $0 \leq j \leq k$ ,  $v_p(f(n+j+u_0 p^{e-v_p(D)/2-1})) \geq i$  if and only if  $v_p(f(n+j)) \geq i$ . Hence the number of terms divisible by  $p^i$  in  $S_{k,f}(n)$  is equal to that in  $S_{k,f}(n+u_0 p^{e-v_p(D)/2-1})$ , i.e.,  $h_{p,i}(n+u_0 p^{e-v_p(D)/2-1}) = h_{p,i}(n)$  for each  $1 \leq i \leq e-1$ . So by (4.19) and (4.23), we get

$$\Delta(n) = h_{p,e}(n + u_0 p^{e-v_p(D)/2-1}) - h_{p,e}(n). \quad (4.24)$$

Define the two sets

$$\mathcal{A}_1(n) := \{f(n), \dots, f(n+d_{p^e}), \dots, f(n+u_0 p^{e-v_p(D)/2-1}-1)\}$$

and

$$\mathcal{A}_2(n) := \{f(n+k+1), \dots, f(n+k+u_0 p^{e-v_p(D)/2-1})\}.$$

Evidently,

$$S_{k,f}(n + u_0 p^{e-v_p(D)/2-1}) \subseteq \mathcal{A}_2(n) \quad (4.25)$$

if  $k < u_0 p^{e-v_p(D)/2-1}$ . If  $k \geq u_0 p^{e-v_p(D)/2-1}$ , then we have the following disjoint unions:

$$S_{k,f}(n) = \mathcal{A}_1(n) \cup \{f(n+u_0 p^{e-v_p(D)/2-1}), \dots, f(n+k)\} \quad (4.26)$$

and

$$S_{k,f}(n + u_0 p^{e-v_p(D)/2-1}) = \{f(n + u_0 p^{e-v_p(D)/2-1}), \dots, f(n + k)\} \cup \mathcal{A}_2(n). \quad (4.27)$$

Claim that there is a positive integer  $n_0$  such that the set  $S_{k,f}(n_0)$  contains exactly two terms divisible by  $p^e$  if  $k < u_0 p^{e-v_p(D)/2-1}$ , while the set  $\mathcal{A}_1(n_0)$  holds exactly two terms divisible by  $p^e$  and the set  $\mathcal{A}_2(n_0)$  has at most one term divisible by  $p^e$ .

Suppose that the claim is true. If  $k < u_0 p^{e-v_p(D)/2-1}$ , then it follows from the claim that

$$h_{p,e}(n_0 + u_0 p^{e-v_p(D)/2-1}) = \max(0, \#\{m \in S_{k,f}(n_0 + u_0 p^{e-v_p(D)/2-1}) : p^e \mid m\} - 1) = 0$$

and

$$h_{p,e}(n_0) = \#\{m \in S_{k,f}(n_0) : p^e \mid m\} - 1 = 1.$$

Hence by (4.24), we get  $\Delta(n_0) = -1$ . If  $k \geq u_0 p^{e-v_p(D)/2-1}$ , then we derive from the claim that

$$h_{p,e}(n_0 + u_0 p^{e-v_p(D)/2-1}) \leq \#\{u_0 p^{e-v_p(D)/2-1} \leq j \leq k : p^e \mid f(n_0 + j)\}$$

and

$$h_{p,e}(n_0) = \#\{u_0 p^{e-v_p(D)/2-1} \leq j \leq k : p^e \mid f(n_0 + j)\} + 1.$$

It follows from (4.24) that  $\Delta(n_0) \leq -1$ . Therefore  $u_0 p^{e-v_p(D)/2-1}$  is not a period of  $g_{p,k,f}$ . Thus Lemma 4.4 is true if  $e > v_p(D)$  and  $v_p(k+1) < e - v_p(D)/2$ . It remains to prove that the claim is true.

First note that by Lemma 2.3 (iii), there are exactly two terms divisible by  $p^e$  in any consecutive  $p^{e-v_p(D)/2}$  terms of the quadratic progression  $\{f(n)\}_{n=1}^\infty$ . Since  $v_p(k+1) < e - v_p(D)/2$ , we can find some integer  $r$  with  $1 \leq r \leq p^{e-v_p(D)/2} - 1$  such that

$$k+1 \equiv r \pmod{p^{e-v_p(D)/2}}.$$

We divide the proof of the claim into the following two cases.

**Case 1.**  $r \in [1, u_0 p^{e-\frac{v_p(D)}{2}-1}]$  with  $u_0 \in [1, \frac{p-1}{2}]$ , or

$$r \in [1, (p-1)p^{e-v_p(D)/2-1}/2] \cup (d_{p^e}, (p+1)p^{e-v_p(D)/2-1}/2]$$

with  $u_0 = \frac{p+1}{2}$ . By Lemma 2.6 we can choose a positive integer  $n_0$  such that  $v_p(f(n_0)) \geq e$  and  $v_p(f(n_0 + d_{p^e})) \geq e$ . By Lemma 2.3 (iii), we know that the terms divisible by  $p^e$  in the quadratic progression  $\{f(n_0 + j)\}_{j \in \mathbb{N}}$  must be of the form  $f(n_0 + t_1 p^{e-v_p(D)/2})$  or  $f(n_0 + d_{p^e} + t_2 p^{e-v_p(D)/2})$ ,  $t_1, t_2 \in \mathbb{N}$ . Since

$$|\mathcal{A}_1(n_0)| = u_0 p^{e-v_p(D)-1} < p^{e-v_p(D)/2}$$

and  $d_{p^e} < u_0 p^{e-v_p(D)/2-1}$ ,  $f(n_0)$  and  $f(n_0 + d_{p^e})$  are the exactly two terms divisible by  $p^e$  in  $\mathcal{A}_1(n_0)$ . On the other hand, since  $k \geq d_{p^e}$  and

$$|S_{k,f}(n_0)| = k+1 \leq u_0 p^{e-v_p(D)/2-1} < p^{e-v_p(D)/2},$$

$f(n_0)$  and  $f(n_0 + d_{p^e})$  are exactly the two terms divisible by  $p^e$  in  $S_{k,f}(n_0)$  if  $k < u_0 p^{e-v_p(D)/2-1}$ . Namely,  $\mathcal{A}_1(n_0)$  holds exactly two terms divisible by  $p^e$  and  $S_{k,f}(n_0)$  contains exactly two terms divisible by  $p^e$  if  $k < u_0 p^{e-v_p(D)/2-1}$ . Now we show that  $\mathcal{A}_2(n_0)$  has at most one term divisible by  $p^e$ . Since  $|\mathcal{A}_2(n_0)| = u_0 p^{e-v_p(D)/2-1} < p^{e-v_p(D)/2}$ , there is at most one term of the form  $f(n_0 + t_1 p^{e-v_p(D)/2})$  and there is at most one term of the form  $f(n_0 + d_{p^e} + t_2 p^{e-v_p(D)/2})$  in the set  $\mathcal{A}_2(n_0)$  with  $t_1, t_2 \in \mathbb{N}$ . Therefore, we only need to show that either there is no term of the form  $f(n_0 + t_1 p^{e-v_p(D)/2})$ , or there

is no term of the form  $f(n_0 + d_{p^e} + t_2 p^{e-v_p(D)/2})$  in the set  $\mathcal{A}_2(n_0)$ , where  $t_1, t_2 \in \mathbb{N}$ , which will be done in the following.

If  $r \in [1, u_0 p^{e-\frac{v_p(D)}{2}-1}]$  with  $u_0 \in [1, \frac{p-1}{2}]$ , we have that for all  $1 \leq j \leq u_0 p^{e-v_p(D)/2-1}$ ,

$$k + j \equiv r + j - 1 \not\equiv 0 \pmod{p^{e-v_p(D)/2}}$$

since

$$1 \leq r + j - 1 \leq 2u_0 p^{e-v_p(D)/2-1} - 1 < p^{e-v_p(D)/2} - 1.$$

Hence there is no term of the form  $f(n_0 + t_1 p^{e-v_p(D)/2})$  in the set  $\mathcal{A}_2(n_0)$  with  $t_1 \in \mathbb{N}$ .

If  $r \in [1, (p-1)p^{e-v_p(D)/2-1}/2] \cup (d_{p^e}, (p+1)p^{e-v_p(D)/2-1}/2]$  with  $u_0 = \frac{p+1}{2}$ , we have for all  $1 \leq j \leq u_0 p^{e-v_p(D)/2-1}$  that

$$1 \leq r + j - 1 \leq (p-1)p^{e-v_p(D)/2-1}/2 + u_0 p^{e-v_p(D)/2-1} - 1 = p^{e-v_p(D)/2} - 1$$

if  $r \in [1, (p-1)p^{e-v_p(D)/2-1}/2]$  and that

$$d_{p^e} < r + j - 1 \leq (p+1)p^{e-v_p(D)/2-1} - 1 \leq p^{e-v_p(D)/2} + d_{p^e} - 1$$

if  $r \in (d_{p^e}, (p+1)p^{e-v_p(D)/2-1}/2]$  since

$$d_{p^e} \geq (u_0 - 1)p^{e-v_p(D)/2-1} = \frac{p-1}{2} p^{e-v_p(D)/2-1} \geq p^{e-v_p(D)/2-1}.$$

That is, for all  $1 \leq j \leq u_0 p^{e-v_p(D)/2-1}$ , we have

$$k + j \equiv r + j - 1 \not\equiv 0 \pmod{p^{e-v_p(D)/2}}$$

if  $r \in [1, (p-1)p^{e-v_p(D)/2-1}/2]$  and

$$k + j \equiv r + j - 1 \not\equiv d_{p^e} \pmod{p^{e-v_p(D)/2}}$$

if  $r \in (d_{p^e}, (p+1)p^{e-v_p(D)/2-1}/2]$ . Therefore, there is no term of the form  $f(n_0 + t_1 p^{e-v_p(D)/2})$  in  $\mathcal{A}_2(n_0)$  if  $r \in [1, (p-1)p^{e-v_p(D)/2-1}/2]$  with  $u_0 = \frac{p+1}{2}$ , and there is no term of the form  $f(n_0 + d_{p^e} + t_2 p^{e-v_p(D)/2-1})$  in  $\mathcal{A}_2(n_0)$  if  $r \in (d_{p^e}, (p+1)p^{e-v_p(D)/2-1}/2]$  with  $u_0 = \frac{p+1}{2}$ , where  $t_1, t_2 \in \mathbb{N}$ . So the claim is proved for Case 1.

**Case 2.**  $r \in (u_0 p^{e-\frac{v_p(D)}{2}-1}, p^{e-v_p(D)/2} - 1]$  with  $u_0 \in [1, \frac{p-1}{2}]$ , or

$$r \in ((p+1)p^{e-\frac{v_p(D)}{2}-1}/2, p^{e-v_p(D)/2} - 1] \cup ((p-1)p^{e-v_p(D)/2-1}/2, d_{p^e}]$$

with  $u_0 = \frac{p+1}{2}$ . Then by Lemma 2.6, we can select a positive integer  $n_0$  such that  $v_p(f(n_0 + u_0 p^{e-v_p(D)/2-1} - 1)) = e$  and  $v_p(f(n_0 + u_0 p^{e-v_p(D)/2-1} - 1 - d_{p^e})) \geq e$ . Now by Lemma 2.3 (iii), the terms divisible by  $p^e$  in the quadratic progression  $\{f(n_0 + j)\}_{j \in \mathbb{N}}$  are of the form

$$f(n_0 + u_0 p^{e-v_p(D)/2-1} - 1 + t_1 p^{e-v_p(D)/2}) \quad (4.28)$$

or

$$f(n_0 + u_0 p^{e-v_p(D)/2-1} - 1 - d_{p^e} + t_2 p^{e-v_p(D)/2}), \quad (4.29)$$

where  $t_1, t_2 \in \mathbb{N}$ .

Since  $k + 1 \equiv r \pmod{p^{e-v_p(D)/2}}$ , one may let  $k = r - 1 + t p^{e-v_p(D)/2}$  for some integer  $t \geq 0$ . It follows that  $k \geq r - 1 \geq u_0 p^{e-v_p(D)/2-1}$  if  $r \in (u_0 p^{e-\frac{v_p(D)}{2}-1}, p^{e-v_p(D)/2} - 1]$  with  $u_0 \in [1, \frac{p-1}{2}]$ , or  $r \in ((p+1)p^{e-\frac{v_p(D)}{2}-1}/2, p^{e-v_p(D)/2} - 1]$  with  $u_0 = \frac{p+1}{2}$ . If  $r \in ((p-1)p^{e-v_p(D)/2-1}/2, d_{p^e}]$  with  $u_0 = \frac{p+1}{2}$ , then it follows from  $k \geq d_{p^e}$  and  $r \leq d_{p^e}$  that  $t \geq 1$ . Thus  $k \geq r - 1 + p^{e-v_p(D)/2} \geq u_0 p^{e-v_p(D)/2-1}$ . That is, we always have  $k \geq u_0 p^{e-v_p(D)/2-1}$  in Case 2. Hence to finish the proof of the claim for Case 2, we only need to treat the two sets  $\mathcal{A}_1(n_0)$  and  $\mathcal{A}_2(n_0)$ .

Evidently,  $u_0 p^{e-v_p(D)/2-1} - 1 - d_{p^e} \geq 0$  since  $d_{p^e} < u_0 p^{e-v_p(D)/2-1}$ . Again using the fact  $|\mathcal{A}_1(n_0)| = u_0 p^{e-v_p(D)-1} < p^{e-v_p(D)/2}$ , we know that  $f(n_0 + u_0 p^{e-v_p(D)/2-1} - 1)$  and  $f(n_0 + u_0 p^{e-v_p(D)/2-1} - 1 - d_{p^e})$  are the exactly two terms divisible by  $p^e$  in  $\mathcal{A}_1(n_0)$ .

Since  $|\mathcal{A}_2(n_0)| = u_0 p^{e-v_p(D)/2-1}$ , to show that  $\mathcal{A}_2(n_0)$  has at most one term divisible by  $p^e$ , it is enough to show that either there is no term of the form (4.28), or there is no term of the form (4.29) in the set  $\mathcal{A}_2(n_0)$ , where  $t_1, t_2 \in \mathbb{N}$ .

If either  $r \in (u_0 p^{e-\frac{v_p(D)}{2}-1}, p^{e-v_p(D)/2} - 1]$  with  $u_0 \in [1, (p-1)/2]$ , or  $r \in ((p+1)p^{e-\frac{v_p(D)}{2}-1}/2, p^{e-v_p(D)/2} - 1]$  with  $u_0 = \frac{p+1}{2}$ , then for all  $1 \leq j \leq u_0 p^{e-v_p(D)/2-1}$ , we have

$$u_0 p^{e-v_p(D)/2-1} < r + j - 1 < p^{e-v_p(D)/2} + u_0 p^{e-v_p(D)/2-1} - 1,$$

which implies that

$$k + j \equiv r + j - 1 \not\equiv u_0 p^{e-v_p(D)/2-1} - 1 \pmod{p^{e-v_p(D)/2}}.$$

Hence there is no term of the form (4.28) with  $t_1 \in \mathbb{N}$  in  $\mathcal{A}_2(n_0)$ .

If  $r \in ((p-1)p^{e-v_p(D)/2-1}/2, d_{p^e}]$  with  $u_0 = \frac{p+1}{2}$ , then

$$\begin{aligned} \frac{p-1}{2} p^{e-v_p(D)/2-1} < r + j - 1 &\leq d_{p^e} + \frac{p+1}{2} p^{e-v_p(D)/2-1} - 1 \\ &< p^{e-v_p(D)/2} + \frac{p+1}{2} p^{e-v_p(D)/2-1} - 1 - d_{p^e} \end{aligned}$$

for all  $1 \leq j \leq u_0 p^{e-v_p(D)/2-1}$  since  $d_{p^e} \leq \frac{p^{e-v_p(D)/2}-1}{2}$ . However,

$$\begin{aligned} \frac{p+1}{2} p^{e-v_p(D)/2-1} - 1 - d_{p^e} &< \frac{p+1}{2} p^{e-v_p(D)/2-1} - 1 - \frac{p-1}{2} p^{e-v_p(D)/2-1} \\ &= p^{e-v_p(D)/2-1} - 1 < \frac{p-1}{2} p^{e-v_p(D)/2-1}. \end{aligned}$$

It then follows that

$$k + j \equiv r + j - 1 \not\equiv \frac{p+1}{2} p^{e-v_p(D)/2-1} - 1 - d_{p^e} \pmod{p^{e-v_p(D)/2}}$$

for all  $1 \leq j \leq u_0 p^{e-v_p(D)/2-1}$ . So there is no term of the form (4.29) with  $t_2 \in \mathbb{N}$  in the set  $\mathcal{A}_2(n_0)$ . So the claim is true in Case 2.

This completes the proof of Lemma 4.4.  $\square$

From Lemmas 4.3 and 4.4, we see that  $v_p(P_{p,k,f})$  depends on some nonnegative integer  $e$  satisfying  $d_{p^e} \leq k < d_{p^{e+1}}$ . In other words, we still don't get the explicit value of  $P_{p,k,f}$ . Thus, to determine the exact value of  $P_{p,k,f}$  for those primes  $p \nmid a$ , we need to transform the information on  $e$  into explicit information depending on  $k$  and  $f$ . We have the following results.

**Lemma 4.5.** *Let  $a$  be odd and  $\mathcal{K}_f$  be nonempty. Then for any  $k \in \mathcal{K}_f$ , we have*

$$P_{2,k,f} = \begin{cases} 2^{v_2(B_k)-2v_2(L_k)}, & \text{if } k < 2^{\lfloor \frac{v_2(D)}{2} \rfloor} \text{ and } v_2(k+1) < v_2(L_k), \\ 2^{\lfloor \frac{v_2(D)}{2} \rfloor}, & \text{if } k \geq 2^{\lfloor \frac{v_2(D)}{2} \rfloor}, D_4 \not\equiv 1 \pmod{8} \text{ and } v_2(k+1) < \lfloor \frac{v_2(D)}{2} \rfloor, \\ 2^{v_2(B_k)-v_2(D)-1}, & \text{if } k \geq 2^{\lfloor \frac{v_2(D)}{2} \rfloor} \text{ and } D_4 \equiv 1 \pmod{8}, \\ 1, & \text{otherwise.} \end{cases}$$

*Proof.* Since  $\mathcal{K}_f$  is nonempty and  $k \in \mathcal{K}_f$ , by Lemma 2.12, there is the unique nonnegative integer  $e$  such that  $d_{2^e} \leq k < d_{2^{e+1}}$ . Consider the following three cases.

**Case 1.**  $k < 2^{\lfloor \frac{v_2(D)}{2} \rfloor}$ . Since  $2 \nmid a$ , we have

$$v_2(a^2 i^2) = 2v_2(i) \leq 2(\lfloor \frac{v_2(D)}{2} \rfloor - 1) \leq v_2(D) - 2 < v_2(D)$$

and so  $v_2(a^2 i^2 - D) = 2v_2(i)$  for any integer  $i$  with  $1 \leq i \leq k$ . Hence

$$\max_{1 \leq i \leq k} \{v_2(a^2 i^2 - D)\} = \max_{1 \leq i \leq k} \{2v_2(i)\} = 2v_2(L_k). \quad (4.30)$$

It follows from (1.4) that

$$v_2(B_k) = \max_{1 \leq i \leq k} \{v_2(i(a^2 i^2 - D))\} = \max_{1 \leq i \leq k} \{v_2(i) + v_2(a^2 i^2 - D)\} = \max_{1 \leq i \leq k} \{3v_2(i)\} = 3v_2(L_k). \quad (4.31)$$

By Lemma 2.9 (i), we have  $d_{2^{\lfloor \frac{v_2(D)}{2} \rfloor - 1}} = 2^{\lfloor \frac{v_2(D)}{2} \rfloor}$ . Thus by Lemma 2.7 and  $d_{2^e} \leq k < 2^{\lfloor \frac{v_2(D)}{2} \rfloor}$ , we have

$$e < 2\lfloor \frac{v_2(D)}{2} \rfloor - 1.$$

Notice that by part (i) of Lemma 2.9,  $d_{2^e}$  (resp.  $d_{2^{e+1}}$ ) is the smallest positive root of the congruence  $a^2 x^2 - D \equiv 0 \pmod{2^e}$  (resp.  $a^2 x^2 - D \equiv 0 \pmod{2^{e+1}}$ ). Hence  $2^{e+1} \nmid (a^2 l^2 - D)$  for all positive integers  $l < d_{2^{e+1}}$ . But  $d_{2^e} \leq k < d_{2^{e+1}}$ . Thus

$$\max_{1 \leq i \leq k} \{v_2(a^2 i^2 - D)\} \geq e \text{ and } \max_{1 \leq i \leq k} \{v_2(a^2 i^2 - D)\} < e + 1.$$

Then by (4.30),

$$e = \max_{1 \leq i \leq k} \{v_2(a^2 i^2 - D)\} = 2v_2(L_k).$$

Therefore, by Lemma 4.3 (i) and (4.31), we get that

$$P_{2,k,f} = 2^{\lceil e/2 \rceil} = 2^{v_2(L_k)} = 2^{v_2(B_k) - 2v_2(L_k)}$$

if  $k < 2^{\lfloor \frac{v_2(D)}{2} \rfloor}$  and  $v_2(k+1) < v_2(L_k)$ , and  $P_{2,k,f} = 1$  if  $k < 2^{\lfloor \frac{v_2(D)}{2} \rfloor}$  and  $v_2(k+1) \geq v_2(L_k)$ . Thus Lemma 4.5 is true in this case.

**Case 2.**  $k \geq 2^{\lfloor \frac{v_2(D)}{2} \rfloor}$  and  $D_4 \not\equiv 1 \pmod{8}$ . By parts (i) and (ii) of Lemma 2.9, one knows that  $d_{2^{\lfloor \frac{v_2(D)}{2} \rfloor - 1}} = 2^{\lfloor \frac{v_2(D)}{2} \rfloor}$  and  $d_{2^{\lfloor \frac{v_2(D)}{2} \rfloor}} = \infty$  if  $D_4 \not\equiv 1 \pmod{4}$ , and  $d_{2^{v_2(D)}} = 2^{\frac{v_2(D)}{2}}$  and  $d_{2^{v_2(D)+1}} = \infty$  if  $D_4 \equiv 5 \pmod{8}$ . It then follows from  $d_{2^e} \leq k < d_{2^{e+1}}$  and  $k \geq 2^{\lfloor \frac{v_2(D)}{2} \rfloor}$  that

$$e = \begin{cases} 2\lfloor \frac{v_2(D)}{2} \rfloor - 1, & \text{if } D_4 \not\equiv 1 \pmod{4}, \\ v_2(D), & \text{if } D_4 \equiv 5 \pmod{8}. \end{cases}$$

Thus by Lemma 4.3 (i), we obtain that  $P_{2,k,f} = 2^{\lceil e/2 \rceil} = 2^{\lfloor \frac{v_2(D)}{2} \rfloor}$  if  $k \geq 2^{\lfloor \frac{v_2(D)}{2} \rfloor}$ ,  $D_4 \not\equiv 1 \pmod{8}$  and  $v_2(k+1) < \lfloor \frac{v_2(D)}{2} \rfloor$ , and  $P_{2,k,f} = 1$  if  $k \geq 2^{\lfloor \frac{v_2(D)}{2} \rfloor}$ ,  $D_4 \not\equiv 1 \pmod{8}$  and  $v_2(k+1) \geq \lfloor \frac{v_2(D)}{2} \rfloor$ . Lemma 4.5 is true in Case 2.

**Case 3.**  $k \geq 2^{\lfloor \frac{v_2(D)}{2} \rfloor}$  and  $D_4 \equiv 1 \pmod{8}$ . Then  $v_2(D)$  is even and  $v_2(L_k) \geq \frac{v_2(D)}{2}$ . Since  $2^{\frac{v_2(D)}{2}}$  is equal to the smallest positive root of the congruence  $a^2 x^2 - D \equiv 0 \pmod{2^{v_2(D)+3}}$ , we derive from Lemma 2.9 (iii) that  $d_{2^{v_2(D)+2}} = 2^{\frac{v_2(D)}{2}}$ . Hence from Lemma 2.7 and  $d_{2^e} \leq k < d_{2^{e+1}}$ , we can derive that  $e \geq v_2(D) + 2$ . So Lemma 2.13 (i) gives that

$$e = \max_{1 \leq i \leq k} \{v_2(a^2 i^2 - D)\} - 1.$$



It follows from Lemma 4.3 (ii) that

$$v_2(P_{2,k,f}) = e - \frac{v_2(D)}{2} = \max_{1 \leq i \leq k} \{v_2(a^2 i^2 - D)\} - \frac{v_2(D)}{2} - 1.$$

Therefore, to show that  $v_2(P_{2,k,f}) = v_2(B_k) - v_2(D) - 1$ , it suffices to prove that the following is true:

$$v_2(B_k) = \max_{1 \leq i \leq k} \{v_2(a^2 i^2 - D)\} + \frac{v_2(D)}{2}, \quad (4.32)$$

which will be done in what follows.

Let  $i$  be an integer such that  $1 \leq i \leq k$ . Then we have that

$$v_2(i(a^2 i^2 - D)) = v_2(i) + \min(2v_2(i), v_2(D)) < v_2(L_k) + v_2(D) \quad (4.33)$$

if  $v_2(i) < \frac{v_2(D)}{2}$ , and that

$$v_2(i(a^2 i^2 - D)) = v_2(i) + v_2(a^2 i^2 - D) = \frac{v_2(D)}{2} + v_2(a^2 i^2 - D) \quad (4.34)$$

if  $v_2(i) = \frac{v_2(D)}{2}$ , and that

$$v_2(i(a^2 i^2 - D)) = v_2(i) + \min\{v_2(a^2 i^2), v_2(D)\} = v_2(i) + v_2(D) \leq v_2(L_k) + v_2(D) \quad (4.35)$$

if  $v_2(i) > \frac{v_2(D)}{2}$ . Now we claim that

$$\max_{\substack{1 \leq i \leq k \\ v_2(i) = v_2(D)/2}} \{v_2(a^2 i^2 - D)\} \geq v_2(L_k) + \frac{v_2(D)}{2} + 1. \quad (4.36)$$

This is equivalent to show that there is an integer  $i_0 \in [1, k]$  with  $v_2(i_0) = \frac{v_2(D)}{2}$  such that

$$v_2(a^2 i_0^2 - D) \geq v_2(L_k) + \frac{v_2(D)}{2} + 1.$$

If  $v_2(L_k) \leq \frac{v_2(D)}{2} + 2$  and  $D_4 \equiv 1 \pmod{8}$ , then pick  $i_0 = 2^{\frac{v_2(D)}{2}} \in [1, k]$ . Since  $2 \nmid a$ , we have

$$v_2(a^2 (2^{\frac{v_2(D)}{2}})^2 - D) = v_2(D) + v_2(a^2 - D_4) \geq v_2(D) + 3 \geq v_2(L_k) + \frac{v_2(D)}{2} + 1.$$

If  $v_2(L_k) > \frac{v_2(D)}{2} + 2$  and  $D_4 \equiv 1 \pmod{8}$ , then  $v_2(L_k) + \frac{v_2(D)}{2} + 1 > v_2(D) + 3$ . Since the discriminant of  $a^2 x^2 - D$  is  $4a^2 D$  and  $v_2(4a^2 D) = v_2(D) + 2$ , then Lemma 2.2 (iv) applied to the congruence  $a^2 x^2 - D \equiv 0 \pmod{2^{v_2(L_k) + \frac{v_2(D)}{2} + 1}}$ , we can find an integer  $i_0 \in [1, 2^{v_2(L_k)}] \subseteq [1, k]$  satisfying that  $v_2(i_0) = \frac{v_2(D)}{2}$  and

$$a^2 i_0^2 - D \equiv 0 \pmod{2^{v_2(L_k) + \frac{v_2(D)}{2} + 1}}.$$

The claim (4.36) is proved. It follows from (4.33)-(4.36) that

$$v_2(B_k) = \frac{v_2(D)}{2} + \max_{\substack{1 \leq i \leq k \\ v_2(i) = v_2(D)/2}} \{v_2(a^2 i^2 - D)\}. \quad (4.37)$$

On the other hand, since  $v_2(a^2 i^2 - D) < v_2(D)$  if  $v_2(i) < \frac{v_2(D)}{2}$  and  $v_2(a^2 i^2 - D) = v_2(D)$  if  $v_2(i) > \frac{v_2(D)}{2}$ , we have

$$\max_{1 \leq i \leq k} \{v_2(a^2 i^2 - D)\} = \max_{\substack{1 \leq i \leq k \\ v_2(i) = v_2(D)/2}} \{v_2(a^2 i^2 - D)\}. \quad (4.38)$$

Hence (4.32) follows immediately from (4.37) and (4.38). Lemma 4.5 is true for Case 3.

This ends the proof of Lemma 4.5.  $\square$

**Lemma 4.6.** *Let  $\mathcal{K}_f$  be nonempty. Then for any  $k \in \mathcal{K}_f$  and any odd prime  $p$  with  $p \nmid a$ , we have*

$$P_{p,k,f} = \begin{cases} p^{v_p(B_k)-2v_p(L_k)}, & \text{if } k < p^{\lceil \frac{v_p(D)}{2} \rceil} \text{ and } v_p(k+1) < v_p(L_k), \\ p^{\lceil \frac{v_p(D)}{2} \rceil}, & \text{if } k \geq p^{\lceil \frac{v_p(D)}{2} \rceil}, v_p(k+1) < \lceil \frac{v_p(D)}{2} \rceil \\ & \text{and either } 2 \nmid v_p(D) \text{ or } (\frac{D_p}{p}) = -1, \\ p^{v_p(B_k)-v_p(D)}, & \text{if } k \geq p^{\lceil \frac{v_p(D)}{2} \rceil}, v_p(k+1) < v_p(B_k) - v_p(D), \\ & 2 \mid v_p(D) \text{ and } (\frac{D_p}{p}) = 1, \\ 1, & \text{otherwise.} \end{cases}$$

*Proof.* By Lemma 2.12, we can find a unique nonnegative integer  $e$  such that  $d_{p^e} \leq k < d_{p^{e+1}}$  since  $\mathcal{K}_f$  is nonempty and  $k \in \mathcal{K}_f$ . Let  $p$  be an odd prime with  $p \nmid a$ . Then we have by (1.4) that

$$v_p(B_k) = v_p(\text{lcm}_{1 \leq i \leq k} \{i(a^2 i^2 - D)\}) = \max_{1 \leq i \leq k} \{v_p(i(a^2 i^2 - D))\}. \quad (4.39)$$

If  $k < p^{\lceil \frac{v_p(D)}{2} \rceil}$ , then for any integer  $i$  with  $1 \leq i \leq k$ , we have

$$2v_p(i) \leq 2v_p(L_k) \leq 2(\lceil \frac{v_p(D)}{2} \rceil - 1) \leq v_p(D) - 1, \quad (4.40)$$

which implies that  $v_p(a^2 i^2 - D) = 2v_p(i)$ . Hence

$$\max_{1 \leq i \leq k} \{v_p(a^2 i^2 - D)\} = \max_{1 \leq i \leq k} \{2v_p(i)\} = 2v_p(L_k) \quad (4.41)$$

and by (4.39), we have

$$v_p(B_k) = \max_{1 \leq i \leq k} \{v_p(i) + 2v_p(i)\} = 3v_p(L_k).$$

Since  $p \nmid a$ , by Lemma 2.13 (ii), we have  $e = \max_{1 \leq i \leq k} \{v_p(a^2 i^2 - D)\}$ . It then follows from (4.40) and (4.41) that  $e = 2v_p(L_k) < v_p(D)$ . Thus by Lemma 4.4,

$$P_{p,k,f} = p^{\lceil e/2 \rceil} = p^{v_p(L_k)} = p^{v_p(B_k)-2v_p(L_k)}$$

if  $k < p^{\lceil \frac{v_p(D)}{2} \rceil}$  and  $v_p(k+1) < v_p(L_k)$ , and  $P_{p,k,f} = 1$  if  $k < p^{\lceil \frac{v_p(D)}{2} \rceil}$  and  $v_p(k+1) \geq v_p(L_k)$ . So Lemma 4.6 is true if  $k < p^{\lceil \frac{v_p(D)}{2} \rceil}$ .

In what follows we let  $k \geq p^{\lceil \frac{v_p(D)}{2} \rceil}$ . Then  $v_p(L_k) \geq \lceil \frac{v_p(D)}{2} \rceil$ .

If  $2 \nmid v_p(D)$  or  $(\frac{D_p}{p}) = -1$ , then by parts (i) and (ii) of Lemma 2.10, we have  $d_{p^{v_p(D)}} = p^{\lceil \frac{v_p(D)}{2} \rceil}$  and  $d_{p^{v_p(D)+1}} = \infty$ . Since  $k \geq p^{\lceil \frac{v_p(D)}{2} \rceil}$  and  $d_{p^e} \leq k < d_{p^{e+1}}$ , we obtain by Lemma 2.7 that  $e = v_p(D)$ . It follows from Lemma 4.4 that  $P_{p,k,f} = p^{\lceil e/2 \rceil} = p^{\lceil \frac{v_p(D)}{2} \rceil}$  if  $v_p(k+1) < \lceil \frac{v_p(D)}{2} \rceil$  and  $P_{p,k,f} = 1$  if  $v_p(k+1) \geq \lceil \frac{v_p(D)}{2} \rceil$ . Thus Lemma 4.6 is true if either  $k \geq p^{\lceil \frac{v_p(D)}{2} \rceil}$  and  $2 \nmid v_p(D)$ , or  $k \geq p^{\lceil \frac{v_p(D)}{2} \rceil}$  and  $(\frac{D_p}{p}) = -1$ .

If  $2 \mid v_p(D)$  and  $(\frac{D_p}{p}) = 1$ , then  $\lceil \frac{v_p(D)}{2} \rceil = \frac{v_p(D)}{2}$  and so  $v_p(L_k) \geq \frac{v_p(D)}{2}$ . First, we claim that

$$v_p(B_k) = v_p(D)/2 + \max_{\substack{1 \leq i \leq k \\ v_p(i) = v_p(D)/2}} \{v_p(a^2 i^2 - D)\}. \quad (4.42)$$

Let

$$C_1 := \max_{\substack{1 \leq i \leq k \\ v_p(i) = v_p(D)/2}} \{v_p(i(a^2 i^2 - D))\} \text{ and } C_2 := \max_{\substack{1 \leq i \leq k \\ v_p(i) > v_p(D)/2}} \{v_p(i(a^2 i^2 - D))\}.$$

Since  $C_1 \geq \frac{3v_p(D)}{2}$  and  $v_p(i(a^2i^2 - D)) < \frac{3v_p(D)}{2}$  if  $v_p(i) < \frac{v_p(D)}{2}$ , we have by (4.39) that

$$v_p(B_k) = \max(C_1, C_2). \quad (4.43)$$

It also implies that  $v_p(B_k) \geq \frac{3v_p(D)}{2}$ .

Note that

$$C_2 = \max_{\substack{1 \leq i \leq k \\ v_p(i) > v_p(D)/2}} \{v_p(i)\} + v_p(D) = v_p(L_k) + v_p(D)$$

if  $v_p(L_k) > \frac{v_p(D)}{2}$ . Thus by (4.43), we obtain that

$$v_p(B_k) = \max(C_1, v_p(L_k) + v_p(D)). \quad (4.44)$$

if  $v_p(L_k) > \frac{v_p(D)}{2}$ . If  $v_p(L_k) > \frac{v_p(D)}{2}$ , since the discriminant of  $a^2x^2 - D$  is  $4a^2D$  and  $v_p(4a^2D) = v_p(D)$ , applying Lemma 2.3 (iii) to the congruence  $a^2x^2 - D \equiv 0 \pmod{p^{v_p(L_k) + \frac{v_p(D)}{2}}}$ , we know that there is an integer  $x_0 \in [1, p^{v_p(L_k)}] \subseteq [1, k]$  such that  $v_p(x_0) = \frac{v_p(D)}{2}$  and  $v_p(a^2x_0^2 - D) \geq v_p(L_k) + \frac{v_p(D)}{2}$ . Hence

$$C_1 = \frac{v_p(D)}{2} + \max_{\substack{1 \leq i \leq k \\ v_p(i) = v_p(D)/2}} \{v_p(a^2i^2 - D)\} \geq v_p(L_k) + v_p(D).$$

It then follows from (4.44) that  $v_p(B_k) = C_1$  if  $v_p(L_k) > \frac{v_p(D)}{2}$ . On the other hand, there is no integer  $i \in [1, k]$  such that  $v_p(i) > \frac{v_p(D)}{2}$  if  $v_p(L_k) = \frac{v_p(D)}{2}$ . So by (4.43),  $v_p(B_k) = C_1$  if  $v_p(L_k) = \frac{v_p(D)}{2}$ . Thus  $v_p(B_k) = C_1$  if  $k \geq p^{\lceil \frac{v_p(D)}{2} \rceil}$  and  $2 \mid v_p(D)$  and  $(\frac{D_p}{p}) = 1$ . The claim (4.42) is proved.

One can easily check that

$$\max_{1 \leq i \leq k} \{v_p(a^2i^2 - D)\} = \max_{\substack{1 \leq i \leq k \\ v_p(i) = v_p(D)/2}} \{v_p(a^2i^2 - D)\}.$$

It then follows from (4.42) that

$$v_p(B_k) = \frac{v_p(D)}{2} + \max_{1 \leq i \leq k} \{v_p(a^2i^2 - D)\}. \quad (4.45)$$

Hence by Lemma 2.13 (ii) and (4.45), we have

$$e = \max_{1 \leq i \leq k} \{v_p(a^2i^2 - D)\} = v_p(B_k) - \frac{v_p(D)}{2},$$

which implies that  $e - \frac{v_p(D)}{2} = v_p(B_k) - v_p(D) \geq \frac{v_p(D)}{2}$  and so  $e \geq v_p(D)$ . Also we have  $\lceil e/2 \rceil = v_p(D)/2 = e - v_p(D)/2 = v_p(B_k) - v_p(D)$  if  $e = v_p(D)$ . It then follows from Lemma 4.4 that

$$P_{p,k,f} = p^{v_p(B_k) - v_p(D)}$$

if  $v_p(k+1) < v_p(B_k) - v_p(D)$  and  $P_{p,k,f} = 1$  if  $v_p(k+1) \geq v_p(B_k) - v_p(D)$ . So Lemma 4.6 is true if  $k \geq p^{\lceil \frac{v_p(D)}{2} \rceil}$ ,  $2 \nmid v_p(D)$  and  $(\frac{D_p}{p}) = 1$ .

This completes the proof of Lemma 4.6.  $\square$

### 5. Proof of Theorem 1.2 and examples

In this section, we first give the proof of Theorem 1.2 by using Lemmas 3.2, 4.2, 4.5 and 4.6.

*Proof of Theorem 1.2.* By Theorem 3.1, we know that the first part of Theorem 1.2 is true. Now we assume that  $\mathcal{K}_f$  is nonempty and  $k \in \mathcal{K}_f$ . Then  $g_{k,f}$  can be extended to a periodic arithmetic function. In what follows we determine the smallest period  $P_{k,f}$  of  $g_{k,f}$ . Let  $\Delta_{p,k} := v_p(B_k) - v_p(P_{p,k,f})$  for any prime  $p$ . Since by Lemma 3.2,  $P_{p,k,f} \mid p^{v_p(B_k)}$  for any prime  $p$ . Hence  $P_{2,k,f} = 1$  if  $2 \nmid B_k$ . So again by Lemma 3.2, we can derive that

$$P_{k,f} = P_{2,k,f} \prod_{p \neq 2, p \mid B_k} p^{v_p(P_{p,k,f})} = \frac{B_k}{2^{\Delta_{2,k}} \prod_{p \neq 2, p \mid B_k} p^{\Delta_{p,k}}} = \frac{B_k}{E_k F_k}, \quad (5.1)$$

where

$$E_k := 2^{\Delta_{2,k}} \left( \prod_{p \neq 2, p \mid \gcd(a,b)} p^{\Delta_{p,k}} \right) \left( \prod_{p \nmid 2a, p \mid D} p^{\Delta_{p,k}} \right) \left( \prod_{p \nmid 2aD, (\frac{D}{p}) = -1} p^{\Delta_{p,k}} \right) \quad (5.2)$$

and

$$F_k := \left( \prod_{p \mid a, p \nmid 2b} p^{\Delta_{p,k}} \right) \left( \prod_{p \nmid 2aD, (\frac{D}{p}) = 1} p^{\Delta_{p,k}} \right). \quad (5.3)$$

First we treat  $E_k$ . If  $p = 2$ , then we get by Lemmas 4.2 and 4.5 that

$$v_2(P_{2,k,f}) = \begin{cases} v_2(B_k), & \text{if } 2 \mid a, 2 \nmid b \text{ and } v_2(k+1) < v_2(B_k), \\ v_2(B_k) - 2v_2(L_k), & \text{if } 2 \nmid a, k < 2^{\lfloor \frac{v_2(D)}{2} \rfloor} \text{ and } v_2(k+1) < v_2(L_k), \\ \lfloor \frac{v_2(D)}{2} \rfloor, & \text{if } 2 \nmid a, k \geq 2^{\lfloor \frac{v_2(D)}{2} \rfloor}, D_4 \not\equiv 1 \pmod{8} \\ & \text{and } v_2(k+1) < \lfloor \frac{v_2(D)}{2} \rfloor, \\ v_2(B_k) - v_2(D) - 1, & \text{if } 2 \nmid a, k \geq 2^{\lfloor \frac{v_2(D)}{2} \rfloor} \text{ and } D_4 \equiv 1 \pmod{8}, \\ 0, & \text{otherwise.} \end{cases}$$

Thus

$$2^{\Delta_{2,k}} = \xi_2 \quad (5.4)$$

with  $\xi_2$  being defined in (1.6).

If  $p \neq 2$  and  $p \mid \gcd(a,b)$ , then by Lemma 4.2, we have  $v_p(P_{p,k,f}) = 0$  and so  $\Delta_{p,k} = v_p(B_k)$ . Hence

$$\prod_{p \neq 2, p \mid \gcd(a,b)} p^{\Delta_{p,k}} = \prod_{p \neq 2, p \mid \gcd(a,b)} p^{v_p(B_k)}. \quad (5.5)$$

If  $p \nmid 2a$  and  $p \mid D$ , then using Lemma 4.6, we obtain

$$\Delta_{p,k} = \begin{cases} 2v_p(L_k), & \text{if } k < p^{\lceil \frac{v_p(D)}{2} \rceil} \text{ and } v_p(k+1) < v_p(L_k), \\ v_p(B_k) - \lceil \frac{v_p(D)}{2} \rceil, & \text{if } k \geq p^{\lceil \frac{v_p(D)}{2} \rceil}, v_p(k+1) < \lceil \frac{v_p(D)}{2} \rceil \\ & \text{and either } 2 \nmid v_p(D) \text{ or } (\frac{D}{p}) = -1, \\ v_p(D), & \text{if } k \geq p^{\lceil \frac{v_p(D)}{2} \rceil}, v_p(k+1) < v_p(B_k) - v_p(D), \\ & 2 \mid v_p(D) \text{ and } (\frac{D}{p}) = 1, \\ v_p(B_k), & \text{otherwise.} \end{cases}$$

It follows that

$$\prod_{p \nmid 2a, p|D} p^{\Delta_{p,k}} = \prod_{p \nmid 2a, p|D} \eta_p, \quad (5.6)$$

where  $\eta_p$  is defined in (1.7).

If  $p \nmid 2aD$  and  $(\frac{D}{p}) = -1$ , then  $v_p(D) = 0$  and  $D = D_p$ . Hence we have  $k \geq p^{\lceil \frac{v_p(D)}{2} \rceil} = 1$ ,  $v_p(k+1) \geq \lceil \frac{v_p(D)}{2} \rceil$  and  $(\frac{D_p}{p}) = -1$ . It then follows from Lemma 4.6 that  $v_p(P_{p,k,f}) = 0$ , which implies that  $\Delta_{p,k} = v_p(B_k)$ . Therefore

$$\prod_{p \nmid 2aD, (\frac{D}{p}) = -1} p^{\Delta_{p,k}} = \prod_{p \nmid 2aD, (\frac{D}{p}) = -1} p^{v_p(B_k)}. \quad (5.7)$$

Now by (5.2) and (5.4)-(5.7), we get that  $E_k = \frac{B_k}{A_k}$ , where  $A_k$  is defined in (1.5). Thus by (5.1), we have

$$P_{k,f} = \frac{A_k}{F_k}. \quad (5.8)$$

Consequently, we handle  $F_k$ . For this purpose, we first prove the following fact: There is at most one prime  $p$  such that  $v_p(k+1) \geq v_p(B_k) \geq 1$ . Suppose that there are two distinct primes  $p_1$  and  $p_2$  such that  $v_{p_1}(k+1) \geq v_{p_1}(B_k) \geq 1$  and  $v_{p_2}(k+1) \geq v_{p_2}(B_k) \geq 1$ . Then  $k+1$  is composite and so  $p_1 \leq k$  and  $p_2 \leq k$ . Hence for each  $1 \leq j \leq 2$ ,

$$v_{p_j}(k+1) \geq v_{p_j}(B_k) = \max_{1 \leq i \leq k} \{v_{p_j}(i) + v_{p_j}(a^2 i^2 - D)\} \geq \max_{1 \leq i \leq k} \{v_{p_j}(i)\} = v_{p_j}(L_k) \geq 1.$$

But Farhi and Kane [11] showed that there is at most one prime  $p \leq k$  such that  $v_p(k+1) \geq v_p(L_k) \geq 1$ . We arrive at a contradiction. Thus the fact is proved.

Now we turn to  $F_k$ . Let  $p \mid B_k$  be a prime satisfying that either  $p \mid a$  and  $p \nmid 2b$  or  $p \nmid 2aD$  and  $(\frac{D}{p}) = 1$ . Then  $v_p(A_k) = v_p(B_k)$ . It then follows from the above fact that there is at most one prime  $p$  such that  $v_p(k+1) \geq v_p(A_k) \geq 1$ .

For any prime  $p$  satisfying that either  $p \mid a, p \nmid 2b$  and  $v_p(k+1) < v_p(B_k)$ , or  $p \nmid 2aD, (\frac{D}{p}) = 1$  and  $v_p(k+1) < v_p(B_k)$ , by Lemmas 4.2 and 4.6, we deduce that  $v_p(P_{p,k,f}) = v_p(B_k)$  and so

$$\Delta_{p,k} = 0 \quad (5.9).$$

If there is no prime  $p$  satisfying that  $v_p(k+1) \geq v_p(A_k) \geq 1$  and either  $p \mid a$  and  $p \nmid b$  or  $p \nmid 2aD$  and  $(\frac{D}{p}) = 1$ , it then follows from (5.3) and (5.9) that

$$F_k = 1. \quad (5.10)$$

If there is exactly one odd prime  $q$  satisfying that  $v_q(k+1) \geq v_q(A_k) \geq 1$  and either  $q \mid a$  and  $q \nmid b$  or  $q \nmid 2aD$  and  $(\frac{D}{q}) = 1$ , then  $v_q(P_{q,k,f}) = 0$ . Then by (5.9) we have

$$F_k = q^{v_q(B_k)} = q^{v_q(A_k)}. \quad (5.11)$$

Thus (5.8) together with (5.10) and (5.11) concludes that  $P_{k,f} = A_k$  except that  $v_q(k+1) \geq v_q(A_k) \geq 1$  for at most one odd prime  $q$  such that either  $q \mid a$  and  $q \nmid b$  or  $q \nmid 2aD$  and  $(\frac{D}{q}) = 1$ , in which case one has  $P_{k,f} = A_k / q^{v_q(A_k)}$ .

The proof of Theorem 1.2 is complete.  $\square$

Now we give some examples to illustrate Theorem 1.2.

**Example 5.1.** Let  $f(x) = 4^l x^2 + 1$  with  $l \geq 1$  being an integer. Then  $D = -4^{l+1}$ ,  $\mathcal{K}_f = \mathbb{N}^*$  and  $Z_{k,f}$  is empty for all integers  $k \geq 1$ . By Theorem 1.2,  $g_{k,f}$  is periodic for all integers  $k \geq 1$ . We have by (1.4),  $B_k := \text{lcm}_{1 \leq i \leq k} \{i(16^l i^2 + 4^{l+1})\}$ . Since

$2 \mid 4^l = \gcd(a, b)$ , we obtain  $\xi_2 = 2^{v_2(B_k)}$  by (1.6). Clearly, there is no odd prime  $p$  such that  $p \mid \gcd(a, b)$  or  $p \mid D$ . On the other hand, all the primes satisfying  $(\frac{-4^{l+1}}{p}) = 1$  are of the form  $p \equiv 1 \pmod{4}$ , and all the primes such that  $(\frac{-4^{l+1}}{p}) = -1$  must be of the form  $p \equiv 3 \pmod{4}$ . Hence by (1.5), we have

$$A_k := \frac{B_k}{2^{v_2(B_k)} \prod_{p \equiv 3 \pmod{4}} p^{v_p(B_k)}}.$$

By Theorem 1.2, the smallest period of  $g_{k,f}$  equals  $A_k$  except that  $v_p(k+1) \geq v_p(A_k) \geq 1$  for at most one prime  $p \equiv 1 \pmod{4}$ , in which case its smallest period is equal to  $\frac{A_k}{p^{v_p(A_k)}}$ .

**Example 5.2.** Let  $f(x) = x^2 + 7 \cdot 4^l$  with  $l \geq 0$  being an integer. Then  $D = -7 \cdot 4^{l+1}$ ,  $\mathcal{K}_f = \mathbb{N}^*$  and  $Z_{k,f}$  is empty for all integers  $k \geq 1$ . By (1.4),  $B_k := \text{lcm}_{1 \leq i \leq k} \{i(i^2 + 7 \cdot 4^{l+1})\}$ . Since  $v_2(D) = 2l + 2$ ,  $D_4 \equiv 1 \pmod{8}$  and  $v_7(D) = 1$ , by (1.6) and (1.7), we get

$$\xi_2 = \begin{cases} 2^{2v_2(L_k)}, & \text{if } k < 2^{l+1} \text{ and } v_2(k+1) < v_2(L_k), \\ 2^{v_2(B_k)}, & \text{if } k < 2^{l+1} \text{ and } v_2(k+1) \geq v_2(L_k), \\ 2^{2l+3}, & \text{if } k \geq 2^{l+1} \end{cases}$$

and

$$\eta_7 = \begin{cases} 7^{v_7(B_k)-1}, & \text{if } k = 7l' + r \text{ with } l' \geq 1 \text{ and } r = 0, \dots, 5, \\ 7^{v_7(B_k)}, & \text{if either } k \leq 6 \text{ or } k = 7l' + 6 \text{ with } l' \geq 1. \end{cases}$$

By some computations, we find that all the odd primes  $p$  such that  $(\frac{-7 \cdot 4^{l+1}}{p}) = 1$  are of the form  $p \equiv 1, 9, 11, 15, 23, 25 \pmod{28}$ , while all the primes with  $(\frac{-7 \cdot 4^{l+1}}{p}) = -1$  are of the form  $p \equiv 3, 5, 13, 17, 19, 27 \pmod{28}$ . Evidently, there is no odd prime  $p$  such that  $p \mid a$ . Thus by Theorem 1.2, the smallest period of  $g_{k,f}$  is equal to

$$A_k := \frac{B_k}{\xi_2 \eta_7 \prod_{p \equiv 3, 5, 13, 17, 19, 27 \pmod{28}} p^{v_p(B_k)}}$$

except that  $v_p(k+1) \geq v_p(A_k) \geq 1$  for at most one odd prime  $p$  of the form  $p \equiv 1, 9, 11, 15, 23, 25 \pmod{28}$ , in which case its smallest period equals  $\frac{A_k}{p^{v_p(A_k)}}$ .

**Example 5.3.** Let  $f(x) = (x+m)(x+m+l)$  with  $m \geq 0$  and  $l \geq 2$  being integers. Then  $D = l^2$  and  $\mathcal{K}_f = \{1, \dots, l-1\}$ . By Theorem 1.2,  $g_{k,f}$  can be extended to a periodic function if and only if  $1 \leq k \leq l-1$ . Now let  $1 \leq k \leq l-1$ . Then by (1.4),

$$B_k = \text{lcm}_{1 \leq i \leq k} \{i(a^2 i^2 - D)\} = \text{lcm}_{1 \leq i \leq k} \{i(l^2 - i^2)\}.$$

Since  $D_4 = \frac{l^2}{2^{2v_2(l)}} \equiv 1 \pmod{8}$  and  $v_q(D) = 2v_q(l)$  for any prime factor  $q$  of  $D$ , we have by (1.6) and (1.7) that

$$\xi_2 = \begin{cases} 2^{2v_2(L_k)}, & \text{if } k < 2^{v_2(l)} \text{ and } v_2(k+1) < v_2(L_k), \\ 2^{v_2(B_k)}, & \text{if } k < 2^{v_2(l)} \text{ and } v_2(k+1) \geq v_2(L_k), \\ 2^{2v_2(l)+1}, & \text{if } k \geq 2^{v_2(l)} \end{cases}$$

and

$$\eta_p = \begin{cases} p^{2v_p(L_k)}, & \text{if } k < p^{v_p(l)} \text{ and } v_p(k+1) < v_p(L_k), \\ p^{2v_p(l)}, & \text{if } k \geq p^{v_p(l)} \text{ and } v_p(k+1) < v_p(B_k) - 2v_p(l), \\ p^{v_p(B_k)}, & \text{otherwise.} \end{cases}$$

Moreover,  $(\frac{D}{p}) = (\frac{l^2}{p}) = 1$  for any prime  $p$  with  $p \nmid 2aD$  and there is no odd prime  $p$  such that  $p \mid \gcd(a, b)$ . It then follows from (1.5) that

$$A_k = \frac{B_k}{\xi_2 \left( \prod_{p \neq 2, p \mid l} \eta_p \right)}.$$

Thus by Theorem 1.2, the smallest period of  $g_{k,f}$  is equal to  $A_k$  except that  $v_p(k+1) \geq v_p(A_k) \geq 1$  for at most one odd prime  $p$  with  $p \nmid 2D$ , in which case its smallest period equals  $\frac{A_k}{p^{v_p(A_k)}}$ .

## 6. Asymptotic estimate of $\log \text{lcm}_{0 \leq i \leq k} \{f(n+i)\}$

In this section, we turn our attention to the asymptotic estimate of  $\log \text{lcm}_{0 \leq i \leq k} \{f(n+i)\}$  for all quadratic polynomials with integer coefficients as  $n$  tends to infinity. We have the following result.

**Theorem 6.1.** *Let  $k$  be a positive integer. Let  $f(x) = ax^2 + bx + c$  be a quadratic polynomial with integer coefficients and let  $D := b^2 - 4ac$ .*

(i). *If  $D \neq a^2 i^2$  for all  $1 \leq i \leq k$ , then the following asymptotic formula holds:*

$$\log \text{lcm}_{0 \leq i \leq k} \{f(n+i)\} \sim 2(k+1) \log n \quad \text{as } n \rightarrow \infty.$$

(ii). *If  $f(x)$  is a quadratic polynomial with integer coefficients such that  $D = a^2 i_0^2$  for some integer  $i_0$  with  $1 \leq i_0 \leq k$ , then we have*

$$\log \text{lcm}_{0 \leq i \leq k} \{f(n+i)\} \sim (k+i_0+1) \log n \quad \text{as } n \rightarrow \infty.$$

*Proof.* It is clear that if  $\gcd(a, b, c) = d$ , then

$$\log \text{lcm}_{0 \leq i \leq k} \{f(n+i)\} = \log \text{lcm}_{0 \leq i \leq k} \{f_1(n+i)\} + O(1),$$

where  $f_1(x) = f(x)/d$  is a primitive polynomial. So without loss of generality, we assume that  $\gcd(a, b, c) = 1$  and  $a > 0$  in what follows.

(i). Since  $D \neq a^2 i^2$  for all  $1 \leq i \leq k$ ,  $\mathcal{K}_f$  is nonempty and  $k \in \mathcal{K}_f$ . By Theorem 1.2, we know that  $g_{k,f}$  can be extended to a periodic arithmetic function. So there is a positive integer  $n_0$  such that for all positive integers  $n \geq n_0$ , we have

$$g_{k,f}(n) \leq M := \max_{1 \leq m \leq P_{k,f}} \{g_{k,f}(n_0 + m)\}.$$

Hence for sufficiently large  $n$ ,

$$\log \left( \prod_{i=0}^k |f(n+i)| \right) - \log M \leq \log \text{lcm}_{0 \leq i \leq k} \{f(n+i)\} \leq \log \left( \prod_{i=0}^k |f(n+i)| \right). \quad (6.1)$$

Since

$$\log \left( \prod_{i=0}^k |f(n+i)| \right) = 2(k+1) \log n + \sum_{i=0}^k \log \left( a + \frac{2ai+b}{n} + \frac{ai^2+bi+c}{n^2} \right)$$

for sufficiently large  $n$ , one has

$$\lim_{n \rightarrow \infty} \frac{\log \left( \prod_{i=0}^k |f(n+i)| \right)}{2(k+1) \log n} = 1 \quad (6.2)$$

and

$$\lim_{n \rightarrow \infty} \frac{\log \left( \prod_{i=0}^k |f(n+i)| \right) - \log M}{2(k+1) \log n} = 1. \quad (6.3)$$

Thus we have by (6.1)-(6.3) that

$$\lim_{n \rightarrow \infty} \frac{\log \text{lcm}_{0 \leq i \leq k} \{f(n+i)\}}{2(k+1) \log n} = 1$$

as desired.

(ii). Since  $D = a^2 i_0^2$  for some integer  $i_0$  with  $1 \leq i_0 \leq k$ ,  $f(x)$  is reducible. It then follows from the proof of Theorem 3.1 that  $f(x)$  must be of the form  $(a_1 x + b_1)(a_1 x + b_1 + a_1 i_0)$  for some integers  $a_1 > 0$  and  $b_1$  with  $\gcd(a_1, b_1) = 1$ . Thus

$$\text{lcm}_{0 \leq i \leq k} \{f(n+i)\} = \text{lcm}_{0 \leq i \leq k} \{(a_1(n+i) + b_1)(a_1(n+i+i_0) + b_1)\}.$$

It is easy to see  $\{a_1(x+i) + b_1\}_{0 \leq i \leq k+i_0}$  is equal to the set of all the linear factors of  $\prod_{i=0}^k f(x+i)$ . Hence  $\text{lcm}_{0 \leq i \leq k+i_0} \{a_1(n+i) + b_1\}$  divides  $\text{lcm}_{0 \leq i \leq k} \{f(n+i)\}$ . So we get that

$$\text{lcm}_{0 \leq i \leq k+i_0} \{a_1(n+i) + b_1\} \leq \text{lcm}_{0 \leq i \leq k} \{f(n+i)\} \leq \prod_{0 \leq i \leq k+i_0} (a_1(n+i) + b_1)$$

for sufficiently large integer  $n$ .

If  $b_1 \geq 0$ , then as in [16], we define the following arithmetic function

$$g_{k+i_0, a_1, b_1}(n) := \frac{\prod_{0 \leq i \leq k+i_0} (a_1(n+i) + b_1)}{\text{lcm}_{0 \leq i \leq k+i_0} \{a_1(n+i) + b_1\}}. \quad (6.4)$$

Then by Theorem 1.2 of [16],  $g_{k+i_0, a_1, b_1}$  is a periodic arithmetic function. So there is a fixed positive integer  $M$  such that  $g_{k+i_0, a_1, b_1}(n) \leq M$  for all positive integers  $n$ . If  $b_1 < 0$ , then we make a revision to the above argument by defining  $\tilde{g}_{k+i_0, a_1, b_1}$  as follows

$$\tilde{g}_{k+i_0, a_1, b_1}(n) := g_{k+i_0, a_1, b_1}(n - b_1).$$

Then Theorem 1.2 of [16] tells us that  $\tilde{g}_{k+i_0, a_1, b_1}$  is a periodic arithmetic function. Thus there exists a fixed positive integer  $M$  such that  $\tilde{g}_{k+i_0, a_1, b_1}(n) \leq M$  for all positive integers  $n$ . So  $g_{k+i_0, a_1, b_1}(n) \leq M$  for all positive integers  $n \geq -b_1$ . This concludes that  $g_{k+i_0, a_1, b_1}(n) \leq M$  for all sufficiently large integers  $n$ . Thus we obtain that

$$\frac{\prod_{0 \leq i \leq k+i_0} (a_1(n+i) + b_1)}{M} \leq \text{lcm}_{0 \leq i \leq k} \{f(n+i)\} \leq \prod_{0 \leq i \leq k+i_0} (a_1(n+i) + b_1)$$

for sufficiently large  $n$ . Since

$$\lim_{n \rightarrow \infty} \frac{\log \prod_{0 \leq i \leq k+i_0} (a_1(n+i) + b_1)}{(k+i_0+1) \log n} = 1,$$

we get

$$\lim_{n \rightarrow \infty} \frac{\log \text{lcm}_{0 \leq i \leq k} \{f(n+i)\}}{(k+i_0+1) \log n} = 1$$

as required. This completes the proof of Theorem 6.1.  $\square$



## 7. Remarks and further questions

In concluding this paper, we make the following remarks.

(1). For any polynomial  $h$  of degree  $\geq 3$  with integer coefficients, we can define the similar function  $g_{k,h}$  for any integer  $n \in \mathbb{N}^* \setminus Z_{k,h}$  by  $g_{k,h}(n) := \frac{\prod_{0 \leq i \leq k} h(n+i)}{\text{lcm}_{0 \leq i \leq k} \{h(n+i)\}}$ , where  $Z_{k,h} := \bigcup_{i=0}^k \{n \in \mathbb{N}^* : h(n+i) = 0\}$ . Similarly, one may ask the following natural question: How to characterize  $h$  such that  $g_{k,h}$  can be extended to a periodic arithmetic function? If  $g_{k,h}$  can be extended to a periodic arithmetic function, what is its smallest period? We believe that the minimal distance among the roots of the corresponding congruence should be helpful to attack such smallest period problem. However, the roots of congruences of higher degree should be more complicated. So the smallest period problem for the higher degree case may require an injection of some new ideas.

(2). In Section 6, we get asymptotic formulas of the logarithm of the least common multiple of  $k+1$  consecutive quadratic progression terms  $\log \text{lcm}_{0 \leq i \leq k} \{f(n+i)\}$  as  $n$  tends to infinity. It is not hard to give the asymptotic formula of  $\log \text{lcm}_{0 \leq i \leq k} \{h(n+i)\}$  for polynomial  $h$  of higher degree as  $n$  goes to infinity if the arithmetic function  $g_{k,h}$  is periodic. It will be interesting to give an asymptotic formula of  $\log \text{lcm}_{0 \leq i \leq k} \{h(n+i)\}$  as  $n$  approaches infinity if  $g_{k,h}$  is not periodic.

(3). As mentioned in the introduction section, an old conjecture states that the product of two or more consecutive positive integers is never a perfect power. In 1857, Liouville made some progress toward this conjecture. In 1939, Erdős [7] [8] showed that there is only a finite number of cases in which a product of consecutive integers is a perfect power. The complete solution of this old conjecture was obtained in 1975 by Erdős and Selfridge [9]. We here find that the least common multiple of consecutive positive integers is never a perfect power. That is, we have the following interesting result.

**Theorem 7.1.** *The least common multiple of two or more consecutive positive integers is never a perfect power.*

In order to show Theorem 7.1, we need the following result of Erdős and Selfridge.

**Lemma 7.2.** [9] *Let  $k, l, n$  be integers with  $k \geq 3, l \geq 2$  and  $n+k \geq p^{(k)}$ , where  $p^{(k)}$  is the least prime satisfying  $p^{(k)} \geq k$ . Then there is a prime  $p \geq k$  such that*

$$v_p \left( \prod_{i=1}^k (n+i) \right) \not\equiv 0 \pmod{l}.$$

*Proof of Theorem 7.1.* To show Theorem 7.1, we need to prove that for any given integers  $n \geq 0, k \geq 2, l \geq 2$ , the integer  $\text{lcm}_{1 \leq i \leq k} \{n+i\}$  is not an  $l$ -th power.

If  $k = 2$  and  $n \geq 0$ , then  $\text{lcm}(n+1, n+2) = (n+1)(n+2)$ , which is never an  $l$ -th power for all integers  $n \geq 0$  since it is well known that the product of any two consecutive positive integers is never an  $l$ -th power. Theorem 7.1 is true in this case.

If  $k \geq 3$  and  $0 \leq n \leq k$ , then we claim that

$$v_t(\text{lcm}_{1 \leq i \leq k} \{n+i\}) = 1, \tag{7.1}$$

where  $t$  denotes the largest prime factor of  $\text{lcm}_{1 \leq i \leq k} \{n+i\}$ . It then follows from (7.1) that  $\text{lcm}_{1 \leq i \leq k} \{n+i\}$  is not an  $l$ -th power. Now we prove (7.1). It is easy to check that  $v_t(\text{lcm}_{1 \leq i \leq k} \{n+i\}) = 1$  if  $3 \leq k \leq 5$  and  $n \leq k$ . If  $k \geq 6$ , then any prime between 2 and  $k$  divides  $\text{lcm}_{1 \leq i \leq k} \{n+i\}$ . Clearly,  $t \geq 5$ . By Bertrand's postulate, we

know that there is at least one prime between  $\lfloor \frac{k}{2} \rfloor$  and  $2\lfloor \frac{k}{2} \rfloor$ . So  $t \geq \lfloor \frac{k}{2} \rfloor$ . Suppose that  $v_t(\text{lcm}_{1 \leq i \leq k} \{n+i\}) \geq 2$ . Then  $t^2 | (n+i_0)$  for some  $1 \leq i_0 \leq k$  and so  $t^2 \leq n+k$ . But we have

$$t^2 \geq 5t \geq 5\lfloor \frac{k}{2} \rfloor \geq 2k + \frac{k}{2} - \frac{5}{2} > 2k \geq n+k$$

since  $t \geq 5$ ,  $t \geq \lfloor \frac{k}{2} \rfloor$  and  $k \geq 6$ . We arrive at a contradiction. So we get (7.1) as desired. Theorem 7.1 is proved in this case.

If  $k \geq 3$  and  $n > k$ , then  $n+k > 2k \geq p^{(k)}$  by Bertrand's postulate, where  $p^{(k)}$  is the least prime satisfying  $p^{(k)} \geq k$ . So by Lemma 7.2, we know that there is a prime  $p \geq k$  such that

$$v_p\left(\prod_{i=1}^k (n+i)\right) \not\equiv 0 \pmod{l}. \quad (7.2)$$

It infers that  $p$  divides the product  $\prod_{i=1}^k (n+i)$ . That is, there is at least one term divisible by  $p$  in the set  $\{n+1, \dots, n+k\}$ . Since  $p \geq k$ , any  $k$  consecutive positive integers are pairwise incongruent modulo  $p$ . Hence there is exactly one term divisible by  $p$  in the set  $\{n+1, \dots, n+k\}$ . It then follows that

$$v_p(\text{lcm}_{1 \leq i \leq k} \{n+i\}) = v_p\left(\prod_{i=1}^k (n+i)\right). \quad (7.3)$$

It then follows from (7.2) and (7.3) that

$$v_p(\text{lcm}_{1 \leq i \leq k} \{n+i\}) \not\equiv 0 \pmod{l}.$$

Therefore  $\text{lcm}_{1 \leq i \leq k} \{n+i\}$  is never an  $l$ -th power.

This completes the proof of Theorem 7.1.  $\square$

The problem of the product of consecutive arithmetic progression terms representing perfect power was investigated by Bennent et al. [3], Györy et al. [12], Saradha and Shorey [25] and Shorey and Tijdeman [27]. Inspired by their work, one may consider the problem of representing perfect power by the product of consecutive terms in the sequence  $\{h(i)\}_{i=1}^{\infty}$  with  $h$  being a polynomial of degree  $\geq 2$  with integer coefficients. Another interesting question is to consider the problem of representing power by the least common multiple of consecutive terms in the sequence  $\{h(i)\}_{i=1}^{\infty}$  with  $h$  being a polynomial with integer coefficients. That is, one can search for the integer solutions of the Diophantine equation  $\text{lcm}_{0 \leq i \leq k} \{h(x+i)\} = y^l$  for any given polynomials  $h$  with integer coefficients and any given positive integer  $k$ .

## REFERENCES

- [1] T.M. Apostol, Introduction to analytic number theory, Springer-Verlag, New York, 1976.
- [2] P. Bateman, J. Kalb and A. Stenger, A limit involving least common multiples, Amer. Math. Monthly 109 (2002), 393-394.
- [3] M.A. Bennett, N. Bruin, K. Györy and L. Hajdu, Powers from products of consecutive terms in arithmetic progression, Proc. Lond. Math. Soc. 92 (2006), 273-306.
- [4] P.L. Chebyshev, Memoire sur les nombres premiers, J. Math. Pures Appl. 17 (1852), 366-390.
- [5] P.G.L. Dirichlet, Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendliche viele Primzahlen enthglt. Abhand. Ak. Wiss. Berlin: (1837) 45-81. [Werke, 1: 315-342.]
- [6] W. Duke, J. Friedlander and H. Iwaniec, Equidistribution of roots of a quadratic congruence to prime moduli, Ann. of Math. (2) 141 (1995), 423-441.
- [7] P. Erdős, Note on products of consecutive integers, J. London Math. Soc. 14 (1939), 194-198.
- [8] P. Erdős, Note on the product of consecutive integers II, J. London Math. Soc. 14 (1939), 245-249.

- [9] P. Erdős and J. Selfridge, The product of consecutive integers is never a power, *Illinois J. Math.* 19 (1975), 292-301.
- [10] B. Farhi, Nontrivial lower bounds for the least common multiple of some finite sequences of integers, *J. Number Theory* 125 (2007), 393-411.
- [11] B. Farhi and D. Kane, New results on the least common multiple of consecutive integers, *Proc. Amer. Math. Soc.* 137 (2009), 1933-1939.
- [12] K. Győry, L. Hajdu and Á. Pintér, Perfect powers from products of consecutive terms in arithmetic progression, *Compositio Math.* 145 (2009), 845-864.
- [13] D. Hanson, On the product of the primes, *Canad. Math. Bull.* 15 (1972), 33-37.
- [14] G.H. Hardy and J.E. Littlewood, Some problems of 'Partitio Numerorum.' III: on the expression of a number as a sum of primes, *Acta Math.* 44 (1922), 1-70.
- [15] S. Hong and W. Feng, Lower bounds for the least common multiple of finite arithmetic progressions, *C.R. Acad. Sci. Paris, Ser. I* 343 (2006), 695-698.
- [16] S. Hong and G. Qian, The least common multiple of consecutive arithmetic progression terms, *Proc. Edinburgh Math. Soc.* 54 (2011), 431-441.
- [17] S. Hong, G. Qian and Q. Tan, The least common multiple of a sequence of products of linear polynomials, *Acta Math. Hungar.* 135 (2012), 160-167.
- [18] S. Hong and Y. Yang, On the periodicity of an arithmetical function, *C.R. Acad. Sci. Paris Sér. I* 346 (2008), 717-721.
- [19] L.-K. Hua, *Introduction to number theory*, Springer-Verlag, Berlin Heidelberg, 1982.
- [20] H. Iwaniec, Almost-primes represented by quadratic polynomials, *Invent. Math.* 47 (1978), 171-188.
- [21] N. Koblitz,  *$p$ -Adic numbers,  $p$ -adic analysis and Zeta functions*, GTM 84, Springer-Verlag, New York, 1984.
- [22] M. Nair, On Chebyshev-type inequalities for primes, *Amer. Math. Monthly* 89 (1982), 126-129.
- [23] K. Ramachandra, T. N. Shorey and R. Tijdeman, On Grimm's problem relating to factorization of a block of consecutive integers, *J. Reine Angew. Math.* 273 (1975), 109-124.
- [24] K. Ramachandra, T. N. Shorey and R. Tijdeman, On Grimm's problem relating to factorization of a block of consecutive integers II, *J. Reine Angew. Math.* 288 (1976), 192-201.
- [25] N. Saradha and T. N. Shorey, Almost squares in arithmetic progression, *Compositio Math.* 138 (2003), 73-111.
- [26] N. Saradha and T. N. Shorey, Contributions towards a conjecture of Erdős on perfect powers in arithmetic progression, *Compositio Math.* 141 (2005), 541-560.
- [27] T. N. Shorey and R. Tijdeman, Perfect powers in products of terms in an arithmetic progression, *Compositio Math.* 75 (1990), 307-344.
- [28] A. Toth, Roots of quadratic congruences, *Int. Math. Res. Not.* 14 (2000), 719-739.

YANGTZE CENTER OF MATHEMATICS, SICHUAN UNIVERSITY, CHENGDU 610064, P.R. CHINA AND  
 MATHEMATICAL COLLEGE, SICHUAN UNIVERSITY, CHENGDU 610064, P.R. CHINA

*E-mail address:* sfhong@scu.edu.cn, s-f.hong@tom.com, hongsf02@yahoo.com

CENTER FOR COMBINATORICS, NANKAI UNIVERSITY, TIANJIN 300071, P.R. CHINA

*E-mail address:* qiangy1230@163.com, qiangy1230@gmail.com